ENCLOSURE

SAFETY EVALUATION REPORT

FOR THE

THREE MILE ISLAND NUCLEAR STATION, UNIT 1

SAFETY PARAMETER DISPLAY SYSTEM

I. INTRODUCTION

All holders of operating licenses issued by the Nuclear Regulatory Commission (licensees) and applicants for an operating license 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 (Ref. 1).

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 parameters 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).

Prompt implementation of the SPDS in operating reactors is a design goal of prime importance. The review of the human factors design of the SPDS for operating reactors called for in NUREG-0737, Supplement 1 is designed to avoid delays resulting from the time required for NRC staff review. The NRC staff will not review operating reactor SPDS designs for compliance with the requirements of Supplement 1 of NUREG-0737 prior to implementation unless a pre-implementation review has been specifically requested by licensees. The licensee's Safety Analysis and SPDS Implementation Plan will be reviewed by the NRC staff only to determine if a serious safety question is posed or if the analysis is seriously inadequate. The NRC staff review to accomplish this will be directed at (a) confirming the adequacy of the parameters selected to be displayed to detect critical safety functions, (b) confirming that means are provided to assure that the data displayed are valid, (c) confirming 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 (d) confirming that the SPDS will be suitably isolated from electrical and electronic interference with equipment and sensors that are used in safety systems. If, based on this review, the staff identifies a serious safety question or seriously inadequate analysis, the Director of IE or the Director of NRR may require or direct the licensee to cease implementation.

II. SUMMARY

The staff reviewed the GPU Nuclear Corporation's SPDS Safety Analysis for the Three Mile Island Nuclear Station, Unit 1. We conclude that it is acceptable for the licensee to continue implementing its SPDS Program, but our approval is conditional upon a satisfactory resolution of staff concerns regarding the display of variables which provide unique data to the operator in evaluating critical safety functions, in particular variables for decay heat removal and containment isolation. It is also conditional to a confirmatory review by the staff of the licensee's Design Validation Test Report and to the resolution of an open item on an electrical isolation device. Additionally, the licensee's data validation method should be upgraded.

III. EVALUATION

The GPU Nuclear Corporation submitted, for staff review, a Safety Analysis dealing with the SPDS for Three Mile Island Nuclear Station, Unit 1 (Ref. 2). Because of insufficient information in the Safety Analysis, the staff was unable to complete its review and a request for additional information (Ref. 5) was made. The licensee's response is contained in Reference 6. In addition, the staff conducted a design verification audit of the licensee's SPDS. This Safety Evaluation Report is based on the results from the staff's review of the Safety Analysis, of the additional information submitted, and results from the audit.

A. SPDS DESCRIPTION

The TMI-1 SPDS is a digital computer based system with CRTs and a keyboard as the user interface. Several display formats contain graphic elements of a form which presents process variable versus process variable, for example, pressure versus temperature. The graphic based formats present information on reactivity, core cooling, and primary side heat removal critical safety functions. These graphic display formats contain data on process variables, with the data encoded in a manner to directly portray the process function and to facilitate the safety assessment of the function by an operator. Because of the ease of making the safety assessment of the process function, this SPDS ranks among the best ones assessed by the staff. Other display formats contain data and information in the form of alphanumerics.

B. PARAMETER SELECTION

Section 4.1f 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.

In our evaluation of the licensee's SPDS variables and in our recommendations, we have considered the TMI-1 "Abnormal Transient Operating Guidelines" (ATOG), which was reviewed and approved by the staff (Ref. 4), as a principle technical source of variables important to operational safety. While we found that the variables selected by the licensee do comprise a generally comprehensive list, we noted that several important process variables needed to assess critical safety functions were not contained in the TMI-1 SPDS. The staff stated these concerns in a request for additional information (Ref. 5) to the licensee. Our request for additional information also expressed a concern on the adequacy of the licensee's method for deriving and validating variable selections.

In a submittal dated January 16, 1985 (Reference 6), the licensee responded to staff concerns regarding the TMI-1 SPDS list of variables. For three variables recommended by the staff, the licensee has justified the TMI-1 SPDS as follows:

(a) Steam Generator Level - Steam generator level is included in the TMI-1 SPDS as a secondary parameter in the primary side heat removal critical safety function.

(b) Source and Intermediate Range Neutron Flux Monitors - The licensee stated that for the TMI-1 SPDS, and its modes of operation, Source and Intermediate Range Startup Rate variables perform an equivalent monitoring function. We accept this justification with the condition that the licensee's variable validation program include cases to confirm the adequacy of the indication for a spectrum of reactivity insertion conditions (such as boron dilution, rod withdrawal, and steamline break).

(c) Steamline Radiation - Although the licensee has not indicated that TMI-1 is equipped with steamline radiation monitors, it has described how alternate monitors could be used for various situations which could arise requiring radioactivity control assessment. For the particular situation of monitoring radiation in an already isolated steam generator, the licensee has stated that actions which might be dictated by the radiation assessment would take enough time to permit assessment by sampling (not a part of SPDS). The licensee's discussion indicates that a rapid assessment (SPDS) is not likely to be needed. Considering the TMI-1 design, TMI-1 Emergency Guidelines and procedures, and the licensee's discussion of alternate provisions, we find the justification acceptable with the condition that a NUREG-0800 steam generator tube rupture scenario (with loss of offsite power) be included in the program to validate the TMI-1 SPDS variables list.

Having reviewed the licensee's discussions in Reference 6, we continue to recommend that the licensee either add Decay Heat Removal Flow and Containment Isolation to the list of SPDS variables or further justify their exclusion. The licensee has asserted that the TMI-1 SPDS is designed to operate only in the following modes: (a) power operation, (b) hot standby, (c) hot shutdown, and (d) post-trip initial response, and that DHR flow does not occur during these modes. The licensee states that the TMI-1 SPDS is not designed for the cold shutdown and refueling modes (when DHR flow does occur). While this discussion addresses the utility of DHR flow as an SPDS parameter during normal decay heat removal system operation, it does not address the monitoring of the viability of the heat removal system during the period in which the steam generators are not the mode of decay heat removal (e.g., ECCS long-term mode of cooling).

With regard to containment isolation, the licensee has stated that this function could be monitored (indirectly) by observing the radiation control and RCS integrity critical safety function. We again conclude that containment isolation is an important parameter of use in making a <u>rapid</u> <u>assessment</u> of the "Containment Conditions" Critical Safety Function, and that a determination that known process pathways through containment have been secured is more directly assured by containment isolation status.

C. DISPLAY DATA VALIDATION

The staff evaluated GPU Nuclear Corporation's SPDS design to determine that means are provided in the display system to assure that the data displayed are valid. The staff's evaluation is based on a review of the licensee's response (Ref. 6) to the staff's request for additional information, and on the results of an audit (Appendix A).

The data validation method used in the display consisted of an out of range check on each sensor signal used. Out of range signals were declared invalid and quality coded as bad signals.

The staff considers the data validation method used in the licensee's design as a minimal one at best when compared with other data validation methods used with the industry. Upon further staff discussion with the licensee, the staff learned that GPU Nuclear is developing a data validation method (more extensive than sensor range checks) for implementation at their Oyster Creek Plant. This data validation method or an equivalent should be incorporated into the TMI-1 SPDS. (See Appendix A for further detail.)

D. HUMAN FACTORS PROGRAM

The staff evaluated GPU Nuclear Corporation's SAR for a commitment to a Human Factors Program to ensure that the displayed information can be readily perceived and comprehended so as not to mislead the operator. The staff also evaluated the TMI-1 SPDS design process and human factors engineering during a design verification audit (Appendix A).

Our review of the licensee's documentation on system specifications and detailed design specifications concluded they were adequate and acceptable. We also noted from the documentation that human factors engineering was an integral and active part of the design process.

During the design verification audit, the staff reviewed several display formats within the SPDS. Our review noted that data and information on each of the critical safety functions was uniquely defined and was easily accessed and evaluated by a user. The display formats composed of graphic elements were well done and generally contained cognitive aids which should facilitate a user's pattern recognition skills in identifying unsafe operation. However, we also noted several human engineering discrepancies (see Appendix A for detail). The licensee should evaluate the safety significance of these discrepancies and correct the discrepancies if necessary.

The staff also evaluated the licensee's Verification and Validation (V&V) Program during our audit of the SPDS. Our review of the V&V Plan concluded it was comprehensive and acceptable. Products from the licensee's design verification activities were also audited and found acceptable. Design validation activities were scheduled for completion by October 1, 1985. For confirmatory review, the staff requests the licensee to docket the Design Validation Test Report on the SPDS.

E. ELECTRICAL AND ELECTRONIC ISOLATION

The licensee's SAR did not address the requirement that the SPDS must be suitably isolated from equipment and sensors that are used in safety systems to prevent electrical and electronic interference. The licensee's response to the staff's request for additional information on isolation devices is presented in Reference 6. Additional information on the isolation devices was also obtained during our audit on August 13, 1985. Our safety evaluation addresses the qualification and documentation of the isolation devices between Class IE safety-related systems and the SPDS.

The interface between safety-related instrumentation and the nonsafety-related SPDS (plant computer) is provided via six different types of isolators. The first type is the Bailey 880 system which is an analog system. This system is part of the original plant computer design which was previously reviewed and approved by the staff at the time of licensing.

The second isolation system is a Foxboro Specification 200 system. The Foxboro Specification 200 system is housed within one cabinet and uses Class IE power supply. Each safety related input to this system passes through two separate isolation devices, first a model 2AI-I2V current to voltage converter then through a model 2AO-VAI voltage to current converter. The output from the model 2AO-VAI is then sent to the SPDS.

The input signal to the 2AC-VAI voltage to current converter is applied to a high impedance input buffer amplifier. The output of the buffer is summed along with the bias and feedback signals at the next stage. The output of this summing stage is then applied to the input of another high impedance amplifier used as an integrator. The output of this amplifier is then chopped (interrupted and polarized to appear as an AC signal) and fed to the primary side of the output transformer. The output from this transformer is then amplified and filtered to produce a 4-20 ma dc output signal.

The maximum credible fault defined by the licensee is 120 Vac and 125 Vdc. One of the requirements of an isolator is its ability to withstand a maximum credible fault at its output without allowing the fault to propagate back to the input. The licensee has submitted test documentation for the Foxboro isolators where a 600 Vac fault was applied across the output signal and signal return (transverse mode), and the output signal and common (common mode). The test configuration shows two strip chart recorders used to monitor any degradation of the input signals. One recorder was used to monitor the input of the voltage to current isolator and another recorder was placed where it would measure any interference at the input of the current to voltage isolator. During the 600 Vac fault application testing there was no visible perturbation or signal degradation recorded on the Class 1E safety related input.

The third device is open contacts on a Control Switch (Electroswitch Series 24). These contacts are used to isolate 16 Core Exit Thermocouples (CET) from the plant computer. These 16 CETs are utilized by a redundant incore read-out device Backup Incore Read Out (BIRO) which can be switched directly to the computer via the series 24 Electroswitch. These devices were tested to withstand 2200 Vac applied between open circuit contacts, closed circuit contacts and non-current carrying parts. This test demonstrates that no arcing or damage to the switch occurs and that there is no insulation resistance breakdown (including carbon traces) upon application of the 2200 Vac.

The above isolation devices used in connection with the SPDS are located in a mild environment and are seismically qualified in accordance with the plant licensing basis.

The fourth and fifth devices that were identified in the January 16, 1985 submittal are Rochester Instrument Model SC-1374 and Victoreen 842 series. These devices are used to isolate the Reactor Building Temperatures (RBT) and Radiation Monitoring System (RMS) respectively from the SPDS. During the audit GPUN informed the staff that the RBT and RMS including the 16 RMS subsystems were Non-Class 1E signals and did not require isolation to interface with the SPDS. GPUN also made a commitment to revise their January 16, 1985 submittal to reflect these changes.

The sixth isolation device is a Rochester Instrument Model SC-1302 which is a Voltage to Voltage converter used to isolate the plant variable "Void Fraction" from the SPDS. The test report reviewed during the audit did not contain the necessary information to demonstrate that this device is qualified to protect the safety systems from the maximum credible faults. The licensee has committed to address the adequacy of this device including testing for maximum credible fault applied to the isolator in the transverse mode.

This is an open item and GPUN must provide the following information to NRC for review and approval:

1. Test procedure showing Test Configuration and Acceptance Criteria.

2. Test results to verify that the maximum credible fault was applied to the output of the Model SC-1302 in the transverse mode (between signal and return) and no perturbations were seen on the Class 1E input.

Based on our audit of the above documentation on the first three isolation devices that are used within the TMI-1 design, we conclude that these devices are qualified isolators and are acceptable for interfacing the SPDS with safety systems. We also conclude that this equipment meets the Commission's requirements in NUREG-0737, Supplement 1.

GPUN should revise their January 16, 1985 submittal to reflect the correct list of Class 1E safety variables that interface with the SPDS.

Also, GPUN must provide a test procedure and test results for the Rochester Instrument Model SC-1302 to verify that this device is a qualified isolator.

IV. CONCLUSIONS

The NRC staff reviewed the GPU Nuclear Corporation's TMI-1 Safety Analysis 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 to date, the staff concludes that no serious safety questions are posed by the proposed SPDS and, therefore, implementation may continue.

The following open items have been identified in our review and should be addressed by the licensee:

1. A Human Factors Program was used in the design of the SPDS. However, our design verification audit noted some human engineering discrepancies within the display formats. These should be assessed by the licensee and corrected as necessary.

2. For confirmatory review, the staff requests the licensee to docket the Design Validation Test Report, and to revise the January 16, 1985 submittal to reflect the correct list of Class 1E safety variables that interface with the SPDS. Also, the licensee must provide a test procedure and test results for the Rochester Instrument model SC-1302 to verify that this device is a qualified isolator.

3. The licensee should either add Decay Heat Removal Flow and Containment Isolation to the list of SPDS variables or further justify their exclusion.

In addition to the above open items, the staff notes that TMI-1's current SPDS equipment has minimal means to assure that the data displayed are valid. The licensee is developing a better data validation method for use and implementation at Oyster Creek. The staff strongly encourages GPUN to improve the data validation at TMI-1, perhaps by adopting the plan to be implemented at Oyster Creek.

The conclusion that SPDS implementation may continue does not imply that the SPDS meets or will meet the requirements of Supplement 1 to NUREG-0737. Such confirmation can be made only after a post-implementation audit or when sufficient information is available for the staff to make such a determination.

V. REFERENCES

1. U.S. Nuclear Regulatory Commission, "Clarification of TMI Action Plan Requirements, Requirements For Emergency Response Capability," U.S. NRC Report NUREG-0737, Supplement 1, January 1983. (Also Generic Letter 82-33, dated December 17, 1982.)

2. Letter from H. D. Hukill, GPU Nuclear Corporation, to D. Eisenhut, NRC, Subject: Safety Parameter Display System, NUREG-0737 (Item I.D.2), dated April 30, 1984, with Attachment: "TMI-1 Safety Parameter Display System Safety Analysis," Topical Report 018.

3. Letter from H. D. Hukill, GPU Nuclear Corporation, to J. Stolz, NRC, Subject: TMI-1 Safety Parameter Display System, dated July 7, 1984, with Attachments: "TMI-1 SPDS Implementation Plan," and "Verification and Validation Plan for TMI-1 Safety Parameter Display System."

4. Letter from J. F. Stolz, NRC, to H. D. Hukill, GPU Nuclear Corporation, Subject: Emergency Operating Procedures (EOP) Upgrade Program, dated March 28, 1984.

5. Letter from J. F. Stolz, NRC, to H. D. Hukill, GPU Nuclear Corporation, Subject: Request for Additional Information Concerning the Three Mile Island Unit 1 Safety Parameter Display System, dated October 9, 1984.

6. Letter from H. D. Hukill, GPU Nuclear Corporation, to J. F. Stolz, NRC, Subject: Response to NRC Requests for Additional Information, dated January 16, 1985.

APPENDIX A

RESULTS FROM THE DESIGN VERIFICATION AUDIT OF THE THREE MILE ISLAND UNIT 1 SAFETY PARAMETER DISPLAY SYSTEM

BACKGROUND

The purpose of this appendix is to document the results from the design verification audit. Reference 1 contains an Audit Plan which was used by the staff to conduct the audit. The main topics of the audit plan are: (1) SPDS Design Process and Human Factors Engineering, (2) Design Verification and Validation, and (3) Data Validation. Isolation devices between the SPDS and safety-grade sensors and device qualification were also evaluated at the audit.

The design verification audit was conducted during August 12-14, 1985 at the plant site. The NRC Audit Team consisted of two members of the Human Factors Engineering Branch and one member of the Instrumentation and Control Systems Branch.

SPDS Design Process and Human Factors Engineering

To evaluate this topic, the staff planned to assess:

- SPDS System's Specifications
- Detailed Design Specification
- Computer Code and Data Base
- Display Format
- Display Devices and Display System Interfaces.

The audit results which follow are structured in terms of the above topics.

During the audit, the staff evaluated the following documentation on the SPDS provided by the licensee at the audit site:

GPU Nuclear
Technical Function Standards
ES-004 Human Engineering Guide, TMI-1, October 17, 1983

TDR No. 583
Safety Parameter Display System (SPDS) User Guidelines, January 14, 1985

The human engineering guide provides guidance for selecting TMI-1 control room components, including displays. It contained design guidance for the selection of demarcations, labels, color, character size, abbreviations, etc. for use in display formats. The licensee stated that the human engineering guide was being revised and expanded to reflect the design experience gained in the development of the SPDS. The new version of the human engineering guide was not available for staff audit.

In the review of the existing Human Engineering Guide with display formats within the SPDS, the staff noted that the guidelines did need to be expanded to cover the labels and abbreviations used in the design. We also noted that the guide did serve as an aid to the display's designer.

The staff's review of the licensee's documentation on system specifications and detailed design specifications concluded they were adequate and acceptable. This result was based on the design detail and task analysis

defined for each of the critical safety functions and on the dedicated display formats as a function of plant state, e.g., power operation, post trip forced flow, and post trip natural circulation. We also noted that the type of data presented in the SPDS design reflected a high degree of integration with the Emergency Operations Procedures. We perceive this to be operationally beneficial to control room personnel during response to emergencies. Also, our review of the design documentation concluded that human factors engineering was an active part of the display's design process. Operation's personnel also participated in the design process by providing user comments and feedback on prototype display formats. In addition, we noted the licensee used good judgment in accepting/rejecting operations feedback.

During the audit, the staff also evaluated a report titled:

Three Mile Island - Unit 1, Modcomp Computer - Safety Parameter Display System Number STD-311/27

This report describes the tests performed on the SPDS and the results from the tests. The purpose of the tests were to verify display, hierarchy, alarm and warning setpoints, and to verify the graphics within the display formats.

Based on a short review of the report, it appeared that a reasonable effort was made in testing the system.

Computer Code and Data Base

Because of time constraints, no review of the computer code and data base was performed during the audit.

Display Formats

The staff reviewed several SPDS display formats which were presented by the licensee on a CRT within the Technical Support Center. The object of the review was to evaluate the display for conformance to NRC requirements and for human engineering deficiencies.

Our review noted that data and information on each of the critical safety functions was uniquely defined and was easily accessed and evaluated within the display system. The graphic based display formats titled "REACT/POWER DIST & PRIM SIDE HEAT REMOVAL and PRIMARY SIDE HEAT REMOVAL (P-T PLOT)" did integrate functionally related data in a manner which facilitates control room user monitoring of the plant. In addition, trending of some variables was also performed in the graphic formats and this appeared to be a useful feature. The use of color and the use of boxes to group data and information appeared adequate.

Our review of display formats did note several HEDs. The symbols used to indicate the current position of trended variables were small and similar to each other, thus it was hard to uniquely identify them and the related process variable. We recommend the use of unique, easily identified symbols to minimize human error.

Other HEDs were:

- Design modifications to display formats resulting from operations feedback appeared cluttered when compared to the average density of information displayed,

- misalignments between numbers within a scale and scale markings existed in several display formats,

- no labels for the scales in the P-T PLOT were available; in addition, the values within the pressure scale were nonlinear in spacing.

These HEDs should be assessed by the licensee for safety significance and the HED corrected as necessary.

Interfaces

The scheme used to access display formats appeared reasonable to the staff. A small keyboard served as the interface device. A dedicated, labeled key is used to display a Safety Parameter Display System Menu. The menu contains the critical safety functions; user selection and entry from the menu results in a top level display format for the critical safety function selected. In addition, each display format contains page prompts in the lower right hand corner which are coordinated with page keys on the keyboard.

Design Verification and Validation

The staff's audit of the licensee's SPDS Design Verification and Validation (V&V) concluded it was a comprehensive plan. The design verification tasks consisted of: (1) system requirement verification, and (2) design verification. A system validation test is also a part of the plan. A structure existed for documenting results and resolving problems defined by V&V activities. In addition, the V&V Plan was based on an independent review and evaluation of the SPDS software with respect to the designers of the system.

At the time of the staff's audit, the implementation of the V&V Plan was incomplete. Products from design verification activities were audited and we concluded that the Plan is being properly implemented. Design validation activities are scheduled for completion by October 1, 1985. For confirmatory review, the staff requested the licensee to docket the Design Validation Test Report.

Data Validation

Our audit of the SPDS determined that a method to validate and quality code data existed in the design. In general, the data validation method was an out of range check on each sensor signal used for the SPDS. Out of range signals were declared invalid and quality coded as bad signals. As a result of this coding, invalid data was easily recognized within the display formats of the system.

The staff considered the data validation method minimal, at best, when compared to other data validation methods used within the industry. A comparison of sensor signals which measure the same process variable may be easily achieved with a digital computer.

Subsequent to the audit, the staff held a phone conference (August 8, 1985) with TMI-1 personnel to discuss data validation. The staff learned that GPU Nuclear has undertaken an effort to develop a data validation method for use and implementation at the Oyster Creek plant. The method developed will be considered for implementation into the TMI-1 SPDS.

Electrical and Electronic Isolation

The audit results on this issue are presented in the SER.

REFERENCE

1. Letter from J. F. Stolz, NRC, to H. D. Hukill, GPU Nuclear Corporation, Subject: "Audit Plan for the Three Mile Island Unit 1 Safety Parameter Display System," dated July 9, 1985.