Any questions regarding this audit, or the Clinton SPDS review in general, may be directed to your licensing Project Manager, Byron Siegel.

A. Schwencer, Chief
Licensing Branch No. 2
Division of Licensing

Enclosures: As stated

*LB#2/DL	* LB#2/DL
BSiegel:dh	ASchwencer
02/06/85	02/06/85

*Previous concurrences concurred on by:

Distribution
Docket File
NRC PDR
Local PDR
PRC System
NSIC
EHylton
DGoddard
ACRS (16)
LB#2 Reading
EJordan
RHeischman
BSiegel
GLapinsky
VMoore

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

FEB 8 1985

Docket No.: 50-461

Mr. Frank A. Spangenberg
Director of Nuclear Licensing &
Configuration Management
Clinton Power Station
P.O. Box 306
Mail Code V920
Clinton, Illinois 61727

Dear Mr. Spangenberg:

SUBJECT: DESIGN VERIFICATION AUDIT REPORT FOR THE CLINTON SAFETY PARAMETER DISPLAY SYSTEM

On December 12 and 13, 1984 the NRC staff audited the verification phase of the Safety Parameter Display System (SPDS) design for the Clinton Power Station (CPS), Clinton, Illinois. The results of our audit are enclosed as: Enclosure 1, "Design Verification Audit Results for Clinton Power Station SPDS" Enclosure 2, a Technical Evaluation Report prepared by the staffs' contractor, Science Applications International Corporation (SAIC); Enclosure 3, copies of the hand-outs you provided for the audit presentations; and Enclosure 4, the Clinton Emergency Procedure Guideline that was "walked-through" as part of the audit. Two of the documents that you provided are too voluminous to be reproduced here; they are the CPS "Requirements Document, Revision 1" and the CPS "Design Document, Revision 2.' At the time of the audit, it is my understanding you committed to submitting these two documents on the NRC docket.

During the audit the staff and its contractor observed several deficiencies in the Clinton design that cast some doubt or the adequacy of the design to comply with the provisions of Supplement 1 to NUREG-0737. These are reported in detail in Enclosures 1 and 2.

These deficiencies were discussed with you during the NRC staff preimplementation audit exit interview. In a letter dated December 21, 1984 you submitted an SPDS Action Plan to resolve our audit findings. As per your request a meeting will be held in Bethesda on February 20, 1985 (Phillips Building, P-114 at 9:00 a.m.) to discuss the results of the SPDS Action Plan with the NRC staff.

Any questions regarding this audit, or the Clinton SPDS review in general, may be directed to your licensing Project Manager, Byron Siegel.

A. Schwencer, Chief
Licensing Branch No. 2
Division of Licensing

Enclosures: As stated

cc: See next page

Clinton

Mr. Frank A. Spangenberg
Director of Nuclear Licensing &
Configuration Management
Clinton Power Station
P. O. Box 306
Mail Code V920
Clinton, Illinois 61727

Mr. D. P. Hall
Vice President
Clinton Power Station
P. O. Box 678
Clinton, Illinois, 61727

Mr. H. R. Victor
Manager-Nuclear Station Engineering Dpt.
Clinton Power Station
P. O. Box 678
Clinton, Illinois 61727

Sheldon Zabel, Esquire
Schiff, Hardin & Waite
7200 Sears Tower
233 Wacker Drive
Chicago, Illinois 60606

Mr. Fred Christenson
Resident Inspector
U. S. Nuclear Regulatory Commission
RR 3, Box 229 A
Clinton, Illinois 61727

Mr. R. C. Heider
Project Manager
Sargent & Lundy Engineers
55 East Monroe Street
Chicago, Illinois 60603

Mr. L. Larson
Project Manager
General Electric Company
175 Curtner Avenue, N/C 395
San Jose, California 95125

Mr. Allen Samuelson, Esquire
Assistant Attorney General
Environmental Control Division
Southern Region
500 South Second Street
Springfield, Illinois 62706

Jean Foy, Esquire
511 W. Nevada
Urbana, Illinois 61801

Richard B. Hubbard
Vice President
Technical Associates
1723 Hamilton Ave. - Suite K
San Jose, CA 95125

Enclosure 1

DESIGN VERIFICATION AUDIT RESULTS FOR CLINTON POWER STATION SPDS

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 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 staff evaluation of the SPDS consists of reviews of the applicant's documentation (i.e., Safety Analysis Report and Implementation Plan) and audit meetings/site visits. Three separate audit meetings/site visits, as described below, may be arranged through the Division of Licensing Project Manager. As dictated by the comprehensiveness of the applicant's documentation and the schedule for design and implementation of the SPDS, the objectives of these audits may be met in fewer site visits.

Design Verification Audit

The purpose of this audit/meeting is to obtain additional information required to resolve any outstanding questions about the V&V Program, to confirm that the V&V Program is being correctly implemented, and to audit the results of the V&V activities to date. At this meeting, the applicant should provide a thorough description of the SPDS design process. Emphasis should be placed on how the applicant is assuring that the implemented SPDS will: provide appropriate parameters, be isolated from safety systems, provide reliable and valid data, and incorporate good human engineering practice. To the extent dictated by the completeness of the V&V Program Plan, the HFEB reviewer will arrange for participation of Procedures and Systems Review Branch (PSRB) and Instrumentation and Control Systems Branch (ICSB) reviewers at this meeting.

Design Validation Audit

After review of all documentation, an audit may be conducted to review the as-built prototype or installed SPDS. The purpose of this audit is to assure that the results of the applicant's testing demonstrate that the SPDS meets the functional requirements of the design and to assure that the SPDS exhibits good human engineering practice.

Installation Audit

As necessary, a final audit may be conducted at the site to ascertain that the SPDS has been installed in accordance with the applicant's plan and is functioning properly. A specific concern is that the data displayed reflect the sensor signal which measures the variable displayed. This audit will be coordinated with and may be conducted by the NRC Resident Inspector.

On December 12 and 13, 1984 a Design Verification Audit was conducted for the Clinton Power Station SPDS design. The audit team included George Lapinsky (NRC/Human Factors Engineering Branch), Michael McCoy (NRC/Procedures and Systems Review Branch), Tim O'Donoghue (Science Applications International Corporation) and Gary Bethke (Comex Corporation). The results of that audit are summarized below. Further detail is also provided in the attached Technical Evaluation Report prepared by Science Applications International Corp. (SAIC).

SUMMARY

The staff was briefed by Illinois Power Company (IP) regarding the design process and verification and validation (V&V) of the Clinton design. IP personnel also "walked-through" a scenario in the plant simulator that included the entry conditions and operator actions involved in a secondary containment/radioactivity release control emergency procedure guideline (EPG). During the "walk-through," a static display of the applicant's proposed SPDS was used to demonstrate SPDS functions and characteristics.

Although the applicant has generally followed an acceptable process for verification of the design, the staff observed some aspects of the design, that may jeopardize its functionality and may result in a design that does not comply with the provisions of Supplement 1 to NUREG-0737.

The design that was was audited is a revision of the original design. The applicant verbally committed to providing two documents on the NRC docket that describe the revised design. These documents are titled "Clinton Power Station Safety Parameter Display System Requirements Document, Revision 1" and "Clinton Power Station Safety Parameter Display System and Supporting Displays Design Document, Revision 2."

Based on the results of the audit, the staff has tentatively decided that a validation audit is necessary and will schedule it for some time subsequent to the SPDS validation (currently planned for summer, 1985).

DISCUSSION

The audit results which follow are organized by general subject area. The branch(es) with primary review responsibility for each subject are identified parenthetically.

1.0 Parameter Selection (Procedures and System Review Branch)

The selection of the Clinton SPDS display variables was made by the applicant using Regulatory Guide 1.97, the plant Final Safety Analysis Report (FSAR), the BWR Generic Emergency Procedure Guidelines (EPGs), and NSAC-21. The audit confirmed that the variables selected are consistent with the presently approved BWR EPGs. The revised design, however, does not include variables for the assessment of the Radioactivity Control function. The staff requires that IP add variables to the SPDS that aid operator assessment of radioactivity control, such as containment high radiation and stack noble gas release rate. The staff also had concerns related to the format and availability of some parameters. These concerns are described below in the Section titled "Human Factors."

Regarding the validation of the Clinton parameter set, the IP staff stated that a desk-top validation had been done by the V&V team. This validation consisted of team consideration of transients and accidents included in the FSAR Chapter 15 analysis and WASH-1400, as well as Loss of All Decay Heat Removal and Anticipated Transient Without Scram (ATWS). In addition IP personnel stated that further validation of the parameter set will take place later in two phases: (1) a static walk-through/talk-through of the Emergency Operating Procedures (EOPs) using a non-operational SPDS display, and (2) a dynamic validation of the Clinton control room, including the SPDS, using the plant-specific simulator. Of concern to the staff is scope of the validation effort. The staff understands that IP plans to clarify its validation plan in a later submittal.

1.1 Information Needed to Continue Review

The applicant should provide information on how the plant simulator or installed system will be used to demonstrate the useability of the SPDS. Identify the test cases which will encompass the variable ranges and setpoints for systems actuation and operator actions. Include consideration of variables for beyond design basis events, such as primary containment pressure limit used in the emergency venting procedure and various degrees of system liquid level degradation. The test cases should demonstrate that each selected SPDS parameter is appropriate to assess the safety status of the Critical Functions (i.e., is useable).

An updated list of SPDS parameters should also be provided, including a discussion of the basis for any deletions.

1.2 Conclusion

Based on the staff's review of the Clinton parameter set, IP presentations during the audit, and the observed consistency of the Clinton parameters with approved BWR Emergency Procedure Guidelines, the staff finds the variable selection for Clinton acceptable contingent upon the addition of variables for the assessment of the Radioactivity Control function and subject to final review of the information requested above pertaining to validation and to the validation results.

2.0 Reliability (Instrumentation and Control Systems Branch)

In its presentation the applicant stated that the SPDS is a subsystem of the Process Computer System and, as such, shares many characteristics with it including reliability. It was further stated that the current estimate of availability ranges from 99.81 percent to 99.96 percent. This estimate was calculated on available data for hardware components, using a fault tree methodology. The availability estimates did not take into consideration SPDS data links or software/firmware induced failures. At the time of the audit, an NRC reviewer from the Instrumentation and Control Systems Branch (ICSB) was not available to audit this issue. However, based on the information presented at the time of the audit, it appears that IP has committed to installing a highly reliable system. Information from the audit (Attachment 3) will be reviewed by ICSB and the staff's final conclusions regarding SPDS reliability will be reported in a Safety Evaluation Report (SER) or a Supplement to the Clinton SER.

3.0 Electrical and Electronic Isolation (Instrumentation and Control Systems Branch)

NUREG-0737, Supplement 1 requires the SPDS to be suitably isolated from electrical or electronic interference with equipment and sensors that are in use for safety systems. At the time of the audit, an NRC reviewer from the ICSB was not available to audit this issue. However, IP has provided further information to ICSB by courier. This information will be reviewed and the staff's final conclusions regarding the adequacy of the proposed isolation devices will be reported in a SER or SER Supplement.

4.0 Display Data Validation (Human Factors Engineering Branch)

The method proposed for display data validation is range checking, supplemented by redundant sensor checking if more than one sensor is available (Drywell Pressure only). The data validation scheme uses color-codes, yellow (normal or good confidence) or white (low confidence) based on whether the data:

1. was deleted
2. failed range check
3. is out of scan

4. is undefined
5. has been inserted.

Generally, this data validation methodology is acceptable; however, in the case of Reactor System Integrity, there is only one parameter (Drywell Floor Drain Sump Flow) proposed to represent this Critical Safety Function (CSF); and as the staff understands it, this parameter cannot be subjected to a confidence check. Therefore, the staff recommends that other parameters be evaluated to supplement this parameter so that the operator can rapidly and reliably assess the status of the Reactor System Integrity function. Examples are reactor water level, safety relief valve position, as well as other relevant parameters that may indicate loss of reactor system integrity inside or outside of containment (e.g., as in a loss of coolant through an interfacing system such as the control rod drives).

In addition, the staff recommends that other data validation techniques such as rate of change algorithms and analytical redundancy be considered for use with those parameters that IP considers primary to the SPDS Critical Safety Functions.

4.1 Information Needed to Continue Review

IP responses to the staff's recommendations should be provided.

4.2 Conclusion

The proposed data validation methodology is acceptable. However, since the Reactor System Integrity function is represented by only one variable (of unknown reliability), the staff requires that further action be taken by IP to provide valid and reliable indication of Reactor System Integrity.

5.0 Human Factors (Human Factors Engineering Branch)

The applicant has developed a program to integrate human factors considerations into the SPDS design and to coordinate the design with other initiatives called for in NUREG-0737, Supplement 1, such as EOPs, control room design review, Regulatory Guide 1.97 instrumentation and Technical Support Center (TSC) design. The design was developed without the direct involvement of a human factors specialist; however, it was subsequently reviewed by a multi-disciplinary team using a human factors checklist. The checklist was assembled from NUREG-0700 and NUREG-0835 (draft) with the help of Dr. Charles Hopkins, a human factors specialist from the University of Illinois.

This human factors review identified "significant concerns" that have been reported to the NRC by IP. The three significant concerns reported were: (1) data validation methods do not fulfill the acceptance criteria of draft NUREG-0835, i.e., physical and/or analytical redundancy; (2) radioactivity data is displayed on a separate screen from the SPDS; and (3) the SPDS does

not provide a separate display for each plant mode.

Regarding the IP team's data validation finding, the staff also finds that the methods used could be improved and has made recommendations above in the Section titled, "Display Data Validation." The problem of providing radioactivity data on a separate display was addressed by IP by redesigning the main SPDS display to include "status boxes" which provide an annunciator function for the critical safety functions. The current SPDS design still has no parameters representing Radioactivity Control but does have a status box that uses alarm data from the ARM/PRM rad monitoring system as its input. After seeing this design prototyped in the control room, and after watching a walk-through/talk-through of a Clinton EPG (secondary containment/radioactivity release control), the staff has tentatively concluded that the problem has not been solved and that rad control variables should be added to the SPDS display (see also "Parameter Selection, above).

The last "significant concern," that the SPDS does not provide separate displays for each operating mode, is not considered to be a problem by IP because the parameters selected for display are regarded by the IP staff to be representative of all plant modes. The staff agrees with this position in concept, but will reserve final judgment until the SPDS parameters have been dynamically evaluated in the validation phase of the V&V Program.

The human factors review done by IP also identified "minor concerns." Among these "minor concerns" was inconsistent color-coding. The staff made a special effort to evaluate this problem because the audit was the first opportunity that the staff had to actually observe the display in color. The staff's observations confirmed that the use of color in the Clinton SPDS is a problem, and, further, that as a result of the EPG walk-through/talk-through, the staff concludes that the color-coding problem (in combination with other design deficiencies) may constitute a serious safety problem.

The color-coding problem is not one but five problems:

1. The color-code used (yellow = normal, red = abnormal, white = invalid, cyan = static information, e.g., mimics, boxes, outlines) is inconsistently used within the SPDS. For example, the tick-marks on the bar graphs that denote normal range are green, not yellow. The symbols for containment isolation valve groups turn red or green based on valve position rather than the abnormality or normality of the isolation.

2. The color-codes also violate the stereotypical expectation, i.e., green = go or normal, yellow = caution or abnormal, red = stop or danger.

3. The colors used were not easily discriminable, especially when used in coding text or numbers. White and cyan could not be

discriminated from each other, green and yellow could not be discriminated from each other.

4. Color-coding was used as a primary coding technique for important information but no redundant coding techniques were used to assure that a loss of color (electronic failure, color-blindness) would not result in a loss of information.

5. The specific red color used on the Clinton system was of such low contrast that number strings and text that were colored red (denoting abnormal or emergency conditions) were very difficult to read.

Based on these findings the staff concluded that, given the limited palette of colors available, IP has misused and overused the color-coding concept to the point where serious confusions are probable. For example, the staff observed during the walk-through/talk-through of the EPG that the operator had difficulty with the containment isolation display. The containment isolation display is a horizonal list of numbers, 1 through 11, representing isolation groups. Under each number are the letters "I" and "O," meaning inboard and outboard. The display is normally green denoting valves open. When an isolation occurs, the "I" and/or "O" turn red.

The operator in the walk-through had other expectations for the colors in this display, as well as for the abbreviations. As far as the staff could tell, the operator could not tell that the display was green, because he stated that the display would turn green when the group isolation was complete. He quickly corrected that to red but hesitated again and said that the "I" meant isolated and the "O" meant open. Since the color-meaning error was in the direction of the stereotypical convention (green = go, OK, normal), the most effective resolution appears to be to change the color-code to the conventional meanings. However, given the discriminability problem, the staff feels that IP should consider not using color at all unless a palette of easily discriminable and readable colors can be developed.

Beyond the concerns developed by the IP staff during the V&V process, the staff developed several specific concerns about the "status box" concept proposed by the applicant. In general the concept of using status boxes as cues for changes in parameter status is a good one. It allows the operator to page through several displays without losing an awareness of changes in the status of the critical safety functions. However, the status boxes or alert boxes do not replace the data, variables, or parameters that support the SPDS function. They are only cues that the status has changed. The operator must still be able to access the underlying variables rapidly and reliably.

The Clinton design presents a problem related to the "status box" concept, i.e., all SPDS variables are not continuously displayed, nor are all SPDS variables input to a status box. The staff's position is that SPDS

parameters must be continuously displayed or an alerting mechanism provided so that the operator is aware of changes in parameter status and can easily access the changing parameter. The current design does not comply with this staff position. For example, the "Power Control" status box lacks input for a "failure to scram" condition, e.g., APRM downscale trip within x seconds; containment pressure and secondary containment delta P are not input to any of the status boxes; containment or drywell high radiation and stack noble gas release rate are not displayed nor do they provide inputs to the Radiation Control status box; none of the ARM/PRM variables are easily accessed as witnessed during the EPG walk-through (the staff recommended at the time of the audit that drywell high radiation and stack noble gas release rate be added to the SPDS.) The "AIDS" concept (display only on alert) does not comply with the requirement for continuous display and therefore, the applicant cannot take credit for parameters in the "AIDS" portion of the display unless they are continuously displayed or are provided as inputs to the critical safety function status boxes and are easily accessible to the operator.

On the positive side the staff was told that IP had lately recognized the need to supply an indicator of SPDS failure and was adding a time-clock display to the design. Procedures for operating the SPDS are available. The SPDS is being reviewed as part of the control room review now underway and human engineering discrepancies (HEDs) involving the SPDS, their assessed safety significance, and changes to the SPDS design that are intended to improve deficiencies of the control room will be reported. Design of the Technical Support Center (TSC) has also been coordinated with the SPDS design. The IP staff appeared to be intent on understanding all of the staff's concerns so that directly responsive actions could be taken to resolve the concerns.

5.1 Information Needed to Continue Review

The applicant should provide a listing of HEDs associated with the SPDS that are identified as part of the control room review, an assessment of their safety significance (in terms of likely effect if an error was made), and a description of the proposed resolution. The applicant should also identify any changes to the SPDS that are made to alleviate deficiencies in the control room.

The applicant should provide details concerning SPDS validation/man-in-the-loop testing including operator sample size, a list of transients and events used in the dynamic validation, and validation results.

Responses to the staff's observations and recommendations are needed if early guidance from the staff is desired.

5.2 Conclusions

Although the V&V Program included a human factors review, the staff observed several human factors deficiencies that had not yet been corrected and that could represent serious safety questions in the design. The staff identified its concerns to the personnel at Illinois Power.