APPENDIX A

TECHNICAL EVALUATION REPORT
FOR THE
SAFETY PARAMETER DISPLAY SYSTEM
FOR
ARIZONA PUBLIC SERVICE COMPANY
PALO VERDE NUCLEAR GENERATING STATION
UNITS 1, 2, AND 3

February 24, 1987

G. L. JOHNSON
W. HANSEN (COMEX)

Lawrence Livermore National Laboratory
for the
United States
Nuclear Regulatory Commission

87Ø4Ø9Ø267XA

TECHNICAL EVALUATION REPORT
FOR THE
SAFETY PARAMETER DISPLAY SYSTEM
FOR
ARIZONA PUBLIC SERVICE COMPANY
PALO VERDE NUCLEAR GENERATING STATION
UNITS 1, 2, AND 3

1. BACKGROUND

NUREG-0660 [1] identified the need for power reactor licensees and applicants for operating licenses to provide a Safety Parameter Display System (SPDS) that will display to operating personnel a minimum set of parameters which define the safety status of the plant. This need was confirmed by NRC in NUREG-0737 [2] and Supplement 1 to NUREG-0737 [3]. SPDS requirements in Supplement 1 to NUREG-0737 replaced those in earlier documents.

Included in Supplement 1 to NUREG-0737 is the requirement that the licensee or applicant prepare a written safety analysis for the SPDS and provide this analysis along with the plant specific SPDS implementation plan for NRC review. Criteria for evaluating Safety Parameter Display Systems are contained in Section 18.2 of NUREG-0800 [4], the Standard Review Plan. These criteria address both the review of a specific SPDS design and review of the applicant's or licensee's verification and validation (V&V) program including the program for SPDS design, development, and testing. Results of the NRC evaluation of a SPDS will be documented in a Safety Evaluation Report (SER) or SER Supplement.

This Technical Evaluation Report provides Lawrence Livermore National Laboratory's (LLNLs) evaluation of the Palo Verde Nuclear Generating Station (PVNGS) SPDS with respect to the requirements of Supplement 1 to NUREG-0737, for NRCs use in preparing a Safety Analysis Report. This evaluation was based upon review of Arizona Public Service Company's (APS) SPDS Safety Analysis Report [5] and the results of an onsite audit conducted by NRC on November 18-20, 1986. During this audit NRC was supported by consultants from LLNL, Comex Corporation, and the Idaho National Engineering Laboratory.

2. SAFETY PARAMETER DISPLAY SYSTEM DESIGN OVERVIEW

The PVNGS SPDS is a function of the site Emergency Response Facility Data Acquisition and Display System (ERFDADS). This system is intended to fulfill the information needs for the Emergency Response Facility (ERF), the Technical Support Center (TSC), and the Supplemental Technical Support Center (STSC), as well as providing the SPDS function for all three units at the Palo Verde site. The ERFDADS consoles in the EOF, TSC, and STSC can display data for any of the PVNGS units. The SPDS consoles in the individual units can display SPDS data only for their specific unit.

GLJ:dm/2/25/87

The ERFDADS computer receives SPDS data from three sources in each unit:

- o The unit Data Acquisition System (DAS)
- o The unit Qualified Safety Parameter Display System (QSPDS)
- o The unit Radiation Monitoring System (RMS)

3. ASSESSMENT OF THE VERIFICATION AND VALIDATION PROGRAM

A Verification and Validation (V&V) Program is concerned with the process of specification, design, fabrication, test, and installation associated with overall system software, hardware, and operation. For the SPDS, verification is the review of the requirements to see that the right problem is being solved and review of the design to see that it meets the requirements. Validation is the performance of tests of the integrated hardware and software systems to see that all requirements are met.

The purpose of the V&V portion of the NRC audit of the Palo Verde Nuclear Generating Station was to obtain information about the PVNGS V&V Program, confirm that the V&V Program was correctly implemented, and audit the results of the V&V. The provisions of NUREG-0737, Supplement 1, and the guidance of NUREG-0800, Section 18.2, Appendix A were used as the basis for the audit. NSAC/39 provided additional guidance.

The PVNGS SPDS purchase specification was completed in August of 1981 and first system delivery to Unit 1 was completed in July of 1982, prior to the issue of NUREG-0737, Supplement 1 (in December of 1982). Consequently, the V&V of the PVNGS SPDS design was conducted after the design, installation, and acceptance of the system was completed.

The Verification portion of the program consisted of performing a review of the SPDS requirements as defined in NUREG-0696, NUREG-0737 Supplement 1, against the PVNGS SPDS functional design specification. A matrix was then prepared and each defined requirement was compared with system capablities as determined from design documents, test plans, visual observations of the as-built system, parameter selection validation documentation, and human factors review documentation to verify that all requirements had been satisfied. PVNGS personnel not involved in the preparation of the Design Specification completed the requirement/capability matrix.

The Validation portion of the program was conducted in two phases which overlapped the completion of the plant Emergency Operating Procedures (EOPs). Both phases used operational personnel to evaluate the SPDS displays. The methodology was the programming of a TSC SPDS display with transient data to simulate violations of Critical Safety Functions (CSFs). Three operators familiar with the EOPs individually evaluated the displays. They were assisted in their evaluation by comprehensive written observation debriefing guides. Interview responses were documented.

The transient data were in the form of four scenarios which were selected on the basis that they embodied the majority of the Critical Safety Functions and that they were available from the Nuclear Steam Supply System vendor's transient studies.

The V&V program and a human factors review of the SPDS resulted in a list of "Safety Parameter Observations" (SPOs). Each SPO was evaluated and placed into one of two categories: SPOs which must be corrected to make the system work or meet regulatory requirements (Category A), or SPOs which would be desirable to correct as "plant betterment" items (Category B). All Category A items were corrected by software changes.

Following the correction of Category A SPOs found during Phase 1, a Phase 2 was conducted utilizing the same technique and scenarios, although different operational personnel were involved. Phase 2 also verified the SPDS modifications accomplished as a result of Phase 1. This resulted in additional SPOs. Each of these SPOs was again placed into one of two categories: features which will impact the SPDS function of providing leading indicators of safety function groups to control room operators during abnorma and emergency conditions (Category 1), and features which will not (Category 2). Correction of Category 1 SPOs commenced coincident with the preparation of the PVNGS SPDS SAR.

The following five phases of the V&V plan are those recommended in NSAC/39:

System Requirements Review
Design Review
Performance Validation Test
Field Verification Test
Final Report

The remainder of this section presents a discussion of the PVNGS SPDS Verification and Validation program and LLNL's evaluation of this program with respect to the first four phases recommended by NSAC/39. The V&V final reports and system design documents were the basis for this evaluation.

3.1. SYSTEM REQUIREMENTS REVIEW

3.1.1. Discussion

The requirements review of the PVNGS SPDS was conducted by a team of personnel from the PVNGS Engineering, Licensing, and Operations disciplines. As the original procurement design specification had been prepared by a contractor (Bechtel) and the personnel selected for the team had not been involved in the preparation of the procurement specification, the use of an in-house team assured independence from the original effort. The team utilized the contents of NUREG-0737, Supplement 1, the guidance in NUREG-0696, and the Purchase Specification to prepare a Design Requirements/Capability matrix. Examination of the matrix during the NRC audit indicated that an independent analysis of the SPDS requirements was performed by PVNGS.

3.1.2. LLNL Evaluation

The PVNGS system requirements review fulfills the intent of the guidance provided by Appendix A to Section 18.2 of NUREG-0800.

3.2. DESIGN VERIFICATION

3.2.1. Discussion

The Design Requirements/Capability matrix was also used to verify that each system requirement was properly implemented by the system design and that the implementation was tested during verification or validation testing. The PVNGS SPDS V&V Team utilized design documents (drawings, manuals, etc.) to verify system design. Test plans, test results, visual observation of the installed system, parameter selection validation documentation, and the SPDS human factors review documentation were used to verify the as-built system.

The verification of design portion of the V&V produced 11 Category A "observations" during the Phase 1 portion of the design verification and 25 Category 1 "observations" during Phase 2. These observations were evaluated and the deficiencies identified were then corrected by software changes.

The software design changes were accomplished using the normal plant change procedure. This procedure is in the form of a departmental instruction [6]. The PVNGS change procedures [7, 8] were examined by the NRC Audit Team. These procedures require reviews by all affected plant organizations. However, they are also time consuming. The NRC Audit Team reviewed one software change which changed set point limits. It took almost one year for the process to implement the change (started 7/11/85; finished 7/1/86). PVNGS does have procedures that allow the shift supervisor to make emergency changes that are documented after the fact.

During examination of SPDS displays the NRC Audit Team noted that the system response (update rates and access times) is, in some instances, too slow to aid users in rapidly and reliably determining the safety status of the plant. The system does not respond as fast as the board instrumentation, which prevents it from being used by the operators to rapidly assess the safety condition of the plant. This lowers the operators confidence in the entire system. Review of the "SPDS Review--Technical Document" showed that APS has recognized the system's response as being too slow to provide some data. This observation was also noted by the operators during the validation in both Phase 1 and Phase 2. PVNGS has, and should continue to make design changes to improve system response. However, as the problem appears to be the overloading of the central processor, which must manipulate data from all three plants, hardware upgrades may prove necessary. While APS has recognized the inadequacy of the current system response, the acceptable limits for response times have not been established.

The NRC Audit Team also noted that the Category 2 SPOs, which may be accomplished as plant betterments, have not been entered into the plant change process.

3.2. Evaluation

The Design Verification Review of the PVNGS V&V appears to have been conducted in an acceptable manner. In LLNL's opinion, however, two items must be resolved before the Verification Review can be considered complete. In order to assure acceptable response is achieved, system design goals must be defined and documented. These goals should be based on operational requirements, and the SPDS design should be modified to achieve these goals. APS should track action on Category 2 SPOs via the plant change procedure. The normal reviews inherent in this process should determine the advisability of and schedule for their completion.

3.3. VALIDATION

3.3.1. Discussion

The validation methodology in both phases was the use of scenarios displayed on a TSC SPDS. The SPDS display of these scenarios were analyzed by operators familiar with the symptomatic EOPs and the event oriented Recovery Procedures. The operators were debriefed in-depth using a debriefing guide and the interviews were documented. The interview data collected were evaluated to determine if the operator can properly identify plant deficiencies as intended by the scenario, if the SPDS parameters are correct and sufficient for each safety group, if the displays are too cluttered, if the names/acronyms used reflect the names used by the operators, if the color coding is correct, if the display acquisition method is easy to use, and if the system response is adequate to allow the operator time to evaluate the discrepancy and formulate further action in a timely manner. Comments on additional items such as training were also obtained.

Two operations personnel (a qualified operator and an STA) participated in the presentation to the NRC Audit Team. Both individuals had taken part in the Validation Tests. They believed the Validation methodology to be beneficial and well conducted. Two other operators, who had not taken part in the V&V, were interviewed by the NRC Team primarily to substantiate observations noted from the Validation Test, and to gain a feel for the operator's acceptance of the system. The latter goal could not be reasonably evaluated because the SPDS is not yet approved for operation by the NRC. The interviews did substantiate a Validation Test result that more training is necessary.

The poor response time of the system appeared as a comment in the validation tests in both phases. SPO 25, a Category 2 observation, states "The display refresh time inhibited the ability of the operator to respond in a timely manner." This observation was disposed of by the following response: "Operator response to this observation is that the speed of the displays was irritating, but not inhibiting. Since the display refresh time did not inhibit the operator's ability to respond in a timely manner, APS will review methods (as a plant betterment) available to speed up displays to ensure that display refresh time does not irritate the operator."

Comments made by the two operators who did not participate in the validation test are summarized below:

Operator A--Reactor Operator, Unit 1. Operator A demonstrated his ability to use the SPDS even though it is not operational. He likes the trend plot and often uses it to check the operation of the other units at Palo Verde. He uses the SPDS console located in the STSC for this function because the control room console will not display data from the other units. Because of plant procedures he would have difficulty using the SPDS during an emergency (note that he is not and would not be a prime user of the SPDS). He believes the SPDS is most useful to the STA as a check on the board instrumentation, and is glad it is available in the TSC and EOF. He would like more training on the SPDS. There were no questions on the SPDS on his last licensing examination.

Operator B--Senior Reactor Operator and Shift Supervisor, Unit 2. Operator B recognized that the control room SPDS would be available for his use, but has low confidence in it because of errors he has noted in the non-SPDS (P&ID) portion of the system. He believes it is an "information overload" item. He believes it is good for the TSC and EOF personnel. He would like more training in the system, but feels there is too much training now for the available time. There were no questions on the SPDS in operator B's last licensing examination.

3.3.2. LLNL Evaluation

APS has conducted a reasonable validation of the SPDS given the constraint that the system is not yet operable in the PVNGS Control Room Simulator. LLNL disagrees, however, with the disposition of the system response time problem and recommends that PVNGS define the operational response time requirements, prepare design goals based on these requirements, and modify the SPDS to achieve these goals.

We also noted that the validation test did not validate the SPDS in the true operational environment. The SPDS will be installed in the PVNGS simulator in the future. At that time it is recommended that a re-validation of the SPDS be conducted using simulator scenarios that exercise all Critical Safety Functions and integrate the use of the SPDS with the EOPs and control board instruments.

3.4. FIELD VERIFICATION

3.4.1. Discussion

The NRC Audit Team examined several field test documents, which were used by APS to verify that the installed system met the SPDS requirements. These included the Site Demonstration Test [13] for ERFDADS, the Test Results Report of the ERFDADS Isolation Cabinet Power Supplies [14], and Instrumentation and Control Loop Functional Verification procedure [15].

3.4.2. LLNL Evaluation

LLNL's examination of the field test dccumentation available indicates that PVNGS performed acceptable field verification of the SPDS.

4. ASSESSMENT OF SPDS DESIGN

4.1. "THE SPDS SHOULD PROVIDE A CONCISE DISPLAY ..."

4.1.1. Discussion

A SPDS console is located next to the Control Room Supervisor's console in each PVNGS unit. Two additional SPDS consoles are located in the Supplemental Technical Support Centers (STSC) adjacent to each unit's control room.

The current status of each Critical Safety Function is displayed by a set of six Safety Indicator Blocks (SIBs). The six blocks correspond to the six Critical Safety Functions monitored by the PVNGS SPDS and they are shown on every ERFDADS display that can be accessed by the control room console without the use of a password. Safety Indicator Blocks change color to reflect the current status of their associated CSF.

The user may also choose to display CSF status on the SPDS overview display. This display shows a color coded deviation bar for each CSF. The color coding of the deviation bar corresponds to the Safety Indicator Block's color. Bar length reflects the relative deviation from normal of the CSF parameter that poses the greatest challenge to that safety function. During NRC Audit Team interviews with plant operators one operator indicated that he has difficulty relating the bar length on this display to CSF status. He felt, however, that additional training would overcome this difficulty.

4.1.2. LLNL Evaluation

The PVNGS SPDS satisfies this requirement of Supplement 1 to NUREG 0737.

4.2. "THE SPDS SHOULD ... DISPLAY ... CRITICAL PLANT VARIABLES"

4.2.1. Discussion

The SPDS uses the following parameters to assess Critical Safety Function status.

CSF	Parameter
Reactivity Control	Control Rod Position
	Linear Reactor Power
	Log Reactor Power
	High Pressure Safety Injection Flow
	Low Pressure Safety Injection Flow

Reactor Heat Removal	Subcooling Margin
	The difference between Core Exit Temperature and RCS Hot Leg Temperature
	RCS delta-T
	RCS Hot Leg Temperature
	Reactor Vessel Outlet Plenum Level
	Steam Generator Water Level
	Steam Generator Pressure
Pressure & Inventory Control	Subcooling Margin
	Reactor Vessel Head Level
	Pressurizer Pressure
	Pressurizer Level
	High Pressure Safety Injection Flow
	Low Pressure Safety Injection Flow
Indirect Radiation Release	Plant Vent Stack Radiation
	Condenser Vacuum Exhaust Radiation
	Fuel Building Exhaust Radiation
	Steam Generator Blowdown Radiation
	Essential Cooling Water Radiation
	Control Room Ventilation Intake Radiation
	Normal Cooling Water Radiation
Containment Integrity	Containment Isolation Valve Status
	Containment Pressure
	Containment Spray Flow
	Containment Temperature
	Containment Sump Level
	Containment Radiation
	Refueling Pool Radiation
	Containment Hydrogen Concentration
Maintenance of Vital Auxiliaries	High Pressure Safety Injection Flow
	Low Pressure Safety Injection Flow
	Containment Spray Flow
	Auxiliary Feedwater Flow
	Steam Flow/Feed Flow Mismatch

During the SPDS audit APS stated that PVNGS operating procedures obviate the need to monitor main steam line radiation as part of the Indirect Radiation Release CSF. PVNGS procedures require that steam generator tubes be covered with water whenever steam is being released via secondary safety or relief valves. APS calculations have shown that this procedure will preclude any significant release of radiation to the atmosphere via this path. The existing SPDS inputs are capable of monitoring all other anticipated paths for releasing radiation via the main steam system. The NRC Audit Team noted that the lack of main steam line radiation as a SPDS parameter deprives the SPDS of direct measurement of an important radioactivity control parameter.

In addition to monitoring the above parameters, the SPDS also monitors the status of the reactor coolant pumps and engineered safety feature actuation signals including: reactor trip, containment isolation, safety injection, and main steam line isolation. A number of these status inputs are used in the determination of SPDS alarm setpoints.

SPDS alarm setpoints vary depending upon the plant operating mode as input by the user. If plant conditions appear to be inconsistent with the current SPDS operating mode the SPDS prompts the user to change the SPDS mode.

4.2.2. LLNL Evaluation

The PVNGS SPDS parameter selection will completely satisfy this requirement of Supplement 1 to NUREG 0737 if main steam line radiation is added to the Indirect Radiation Release CSF.

Additionally, LLNL suggests that the system would be improved by displaying Auxiliary Feedwater (AFW) flow as part of the Heat Removal CSF. Although AFW flow is displayed as part of the Vital Auxiliaries CSF, this parameter should be added to the Heat Removal CSF because AFW flow provides rapid indication that heat removal via the steam system is being challenged. Furthermore, this parameter is expected to be used in conjunction with steam generator water level which also appears on Heat Removal CSF displays.

4.3. "THE SPDS SHOULD ... AID THEM (OPERATORS) IN RAPIDLY AND RELIABLY DETERMINING THE SAFETY STATUS OF THE PLANT"

4.3.1. Discussion

The unit Data Acquisition Systems scan each SPDS input at least ten times per second and transmit the current reading of each input to the ERFDADS host computer about once every second. The current value of individual instrument channels directly displayed on the SPDS are updated on a one to three second interval. SPDS parameters that are derived from more than one input are updated every 10 seconds. The length of deviation bars on the first and second-level SPDS displays is also updated every 10 seconds. Deviation bar and SIB color is updated every 20 seconds. Parameter trend plots are updated every 30 seconds with a single value representing the average value of the parameter over the preceding 30 seconds.

The NRC Audit Team witnessed the SPDS engineering and development system being used by a plant operator to monitor the progress of a simulated plant transient. The Audit Team noted that it was possible to monitor CSF status during the course of the simulated transient. The relatively slow update of deviation bars and the status color coding, however, occasionally led to temporary confusion. For example, during the initial 20 seconds following a reactor trip the SPDS displays were interpreted as indicating an Anticipated Transient Without Scram condition. This confusion occurred because of the SPDS's delay in detecting control element assembly position and reactor power, and displaying this information in terms of parameter deviation bars and color color coding, CSF deviation bars and color coding, and Safety Indicator Block color coding.

The value of a SPDS parameter is displayed only on its third-level, trend plot, display. The current parameter value is displayed next to the trend plot. During the simulated transient run-through the LLNL noticed that the SPDS users were frequently switching from the mid-level displays to the trend plots in order to ascertain current parameter values.

SPDS data validation is based upon range checks and interchannel comparison of redundant inputs. For parameters input via the unit DAS, the DAS checks the input voltage or current level against the instrument channel limits. The DAS converts the input to engineering units and transmits the value to the host computer. SPDS parameters that are received via the QSPDS are subject to range checks, engineering units conversion, and interchannel comparison in that unit. Inputs from the Radiation Monitoring System receive validity checking that includes verification of communications link operability, detector response to a check source, and gas sample system flows. Both the QSPDS and the RMS transmit a validity flag to the ERFDADS host computer along with the parameter value. The host computer checks each input against predetermined reasonableness limits and, for redundant inputs, verifies that the inputs agree within a predetermined amount. Data that falls outside of the reasonable limits are considered invalid. Redundant inputs that do not agree within the predetermined amount are both considered invalid.

The NRC Audit Team examined the data validation algorithms for parameters in the Heat Removal CSF. This examination included data validation performed by the QSPDS as well as the ERFDADS host computer. The Audit Team noted that the algorithms used would, in most cases, provide reasonable assurance that questionable data is flagged as such by the SPDS. Review of the data validation algorithms, however, identified that APS did not develop a consistent basis for interchannel comparison validity criteria. For example, steam generator water level inputs are considered valid if they agree within 10 percent. Review of instrument loop accuracy data showed, however, that under harsh containment environments, redundant readings could correctly differ by a greater amount.

Examination of range check limits showed that these limits represent the limits of the process instrumentation rather than reasonable limits of the measured parameter. For example, subcooling margin values are checked to see that they indicate between -714 and +645 degrees F even though credible values of this parameter occupy a much narrower band around 0 degrees F.

When invalid data are encountered the last valid value for the affected parameter is displayed until new validated values are available. This use of the last valid value is flagged on SPDS displays by using question marks as plot points on the parameter trend plots and by displaying the parameter numerical value and deviation bar chart in blue. If any parameter in a CSF group is invalid the overview display bar for that CSF is shown in blue. Safety Indicator Block color does not reflect parameter validity information. The Safety Indicator Block's color always corresponds to the status of the CSF parameter with the greatest deviation form normal, regardless of parameter validity. Thus it is possible for a CSF Safety Indicator Block to show normal even if none of that CSF's input parameters are valid.

Parameter values may be input from the SPDS computer console. This feature is password protected. The ability to change displays or data validation algorithms is also password protected. Revision to SPDS software is controlled by procedure.

SPDS operability is indicated by a clock in the lower right hand corner of all displays and the character Z flashing in the upper left hand corner. The clock updates every second when the SPDS is operating and does not update when the SPDS is inoperable. The flashing Z stops flashing and changes color when the terminal is not communicating with the host computer.

SPDS hardware consists of redundant data acquisition system computers in each unit that feed the common ERFDADS host computers. The host computers are redundant and share a common SPDS parameter data base. The host computers are powered from the battery backed, diesel backed TSC power system. The unit DAS computers are normally powered from offsite power. An automatic transfer switch energizes the unit DAS from a diesel backed bus in the event of the loss of the offsite source. During this transfer DAS power is temporarily interrupted. The loss of power interrupts DAS processing and necessitates downloading the DAS program from the host computer and rebooting the DAS program. This process takes approximately three minutes. Consequently, this arrangement of DAS power results in the SPDS being out of service during the first three minutes of any transient that includes a loss of offsite power.

APS has collected ten months of ERFDADS availability data. Over the period January 1986 to October 1986 the SPDSs for all three PVNGS units exhibited an average availability exceeding 0.99. The worst average monthly availability for any single unit's SPDS was 0.96.

4.3.2. LLNL Evaluation

There are a number of shortcomings that prevent LLNL from concluding that the PVNGS SPDS completely addresses this requirement of Supplement 1 to NUREG-0737.

- The relatively long period for updating the color code of the deviation bars and Safety Indicator Blocks, and for updating the length of deviation bars appears to be a potential source of user confusion.

- It is not clear that the thirty second update rate for the parameter trend plots is consistent with user needs.

- It is not clear that the acceptance limits for the interchannel comparison validity checking are reasonable and based upon consistently applied criteria.

- Invalid data flags do not propagate to the Safety Indicator Blocks. Therefore, the Safety Indicator Blocks may incorrectly indicate CSF status based upon invalid inputs.

- o The selection of power sources for the unit Data Acquisition Systems insures that the SPDS will be inoperable during the first three minutes of any transient that involves the loss of offsite power. Thus, by design, the PVNGS SPDS will not aid operators in rapidly and reliably determining the safety status of the plant during the initial phase of this class of transients.

In order to allow a final positive conclusion about the PVNGS SPDS with respect to this provision of Supplement 1 to NUREG-0737, APS must address the above items. A discussion of APS actions in this regard should be submitted for NRC review.

LLNL recommends that APS's resolution of the concerns with system update rates be based upon a task analysis that identifies operator needs in this regard. This task analysis should address needed time resolution for trend plots as well.

It should be noted that neither 1E power to the DAS nor an expensive, uninterruptable power supply is needed to avoid unit DAS failure as a consequence of loss of offsite power. Rather provision of a relatively inexpensive, off-the-shelf, battery backup for the unit DAS program memory would be sufficient to allow these computers to ride through the momentary interruption in power associated with the transition to diesel power.

In addition to the above items LLNL suggests that APS consider tightening the host computer parameter range checks to values that represent reasonable limits for the process involved rather than instrumentation measurement limitations. This change should improve the overall effectiveness of the SPDS data validity checking.

During the course of the audit it appeared to LLNL that displaying the current value of SPDS parameters on second level displays might also improve SPDS usefulness. We could not, however, judge whether the additional display complexity that would result from this change would detract from the displays more than would be gained by adding parameter values. Therefore, LLNL recommends that APS specifically review this issue after enough operating experience has been gained with the existing system to allow knowledgeable feedback from the system users.

4.4. "THE PRINCIPLE PURPOSE AND FUNCTION OF THE SPDS IS TO AID THE CONTROL ROOM PERSONNEL DURING ABNORMAL AND EMERGENCY CONDITIONS IN DETERMINING THE SAFETY STATUS OF THE PLANT AND IN ASSESSING WHETHER ABNORMAL CONDITIONS WARRANT CORRECTIVE ACTIONS BY CONTROL ROOM OPERATORS TO AVOID A DEGRADED CORE."

4.4.1. Discussion

The placement of plant parameters into CSF groups was based upon review of the PVNGS Emergency Operating Procedures (EOPs) and Functional Recovery Procedures. The "leading" parameters for each safety function, as determined by this review, were grouped into the PVNGS SPDS CSF displays. The NRC Audit Team performed a comparison of the SPDS displays with the EOP decision process used to manually evaluate safety function status. This effort identified numerous differences between the information and logic used by the SPDS to assess safety status, and the information and logic used by the operators to accomplish the same function. Therefore, the PVNGS SPDS is not truly integrated with the rest of the control room, or the plant EOPs.

The status of each CSF parameter is indicated by deviation bar lengths and color code on mid-level displays. Deviation bars extend along a parameter status axis that has equally spaced reference points corresponding to normal, alarm, and unsafe values of deviation. This status axis extends in both directions so that parameter deviations in either the positive or negative direction may be displayed. The length of the deviation bar corresponds to the relative value of the parameter with respect to the status reference points between which the parameter value falls. If, for example, a parameter value lies halfway between the alarm and unsafe limits the end of the deviation bar will be positioned halfway between these reference points. Since the parameter value difference between successive reference points is usually not constant, the absolute change in a parameter value represented by a given incremental change in deviation bar length is dependent upon the parameter alarm status.

Deviation bars are color coded to reflect the parameter's current safety status as follows:

Green	Normal
Yellow	Alarm
Red	Unsafe
Blue	Invalid

CSF status is propagated from the mid-level displays to the overview display by multiplying the absolute bar length for each parameter by a predetermined, mode dependent, weighting factor and plotting the longest resultant on the overview display deviation bar chart.

The weighting factor is 0 or 1 in most cases. A weight of 0 is assigned to parameters that are not germane to the determination of CSF status in the current operating mode. Thus the top-level display CSF deviation bar length equals the length of the mid-level display status bar for the most deviant parameter that is important in the current mode. The one exception to this rule is the linear reactor power parameter which has a weight of 0.5.

Color coding of the overview display bars and the Safety Indicator Blocks follows the same convention as is used on the mid-level displays. In the event that one or more CSF parameters are invalid the deviation bar length is calculated using the last current value of the invalid parameter(s). Overview deviation bars for CSFs with one or more invalid parameters are displayed in blue. Safety Indicator Blocks are never color coded blue. They always show CSF status as determined by using the current or the last valid value of the CSF parameter.

Indication of the ESF actuation signal status and Reactor Coolant Pump status is color coded as follows:

Yellow	ESF signal actuated
Blue	ESF signal not actuated
Red	RCP on
Green	RCP off

The NRC Audit Team noted that the meaning of red, yellow, green, and blue on these status displays is not consistent with their meaning on the deviation bar charts and the Safety Indicator Blocks. The meaning of red and green for RCP status is, however, consistent with the control board convention. APS stated that the use of these colors with different meanings in different portions of the display was forced by system limitations. Their system validation exercises indicated that operator confusion does not result from this inconsistency.

The PVNGS SPDS can display 30 minute historical trend plots of analog SPDS parameters. Each point on the trend represents a 30 second average of the parameter value. The trend displays incorporate an auto-ranging feature that expands the parameter scale to the degree permitted by the deviation over the 30 minute history. Trend plots are oriented with the newest data at the left edge of the plot and the oldest data at the right. This is reversed from the convention used on analog-hardwired trend recorders.

The trend plots do not display current or historical values of parameter normal, alarm, and unsafe setpoints. APS indicated that this had once been a SPDS feature, but that human factors review concluded that inclusion of setpoint plots on the time histories unacceptably cluttered the displays.

The current parameter value is displayed adjacent to the parameter axis on the trend plots. The display text is color coded to indicate the parameter's current safety status. Color coding is consistent with the color coding of mid- and top-level display deviation bars.

4.4.2. LLNL Evaluation

The PVNGS SPDS fully satisfies this requirement of NUREG-0737, Supplement 1. LLNL suggests, however, that one advantage of trend plots over deviation bar charts is that a trend plot allows one to monitor the trend of the margin between the parameter value and the alarm/caution limits. Therefore, the trend plot displays would be more useful if information about alarm limits could be provided without confusing the display. APS might consider alternative approaches to the display of alarm limits such as confining the display to the current value of the the limits immediately above and below the parameter value. This might be combined with a relatively unobtrusive indication of the limits such as numerical display of the limits, or colored marks that indicate the alarm points on the parameter axis and that indicate when the alarm points are offscale.

We also suggest that changing the direction of the trend plot time axis to be consistent with the convention used by analog-hardwired recorders would eliminate a possible source of user confusion.

4.5. "THE SPDS (SHALL BE) LOCATED CONVENIENT TO THE CONTROL ROOM OPERATORS"

4.5.1. Discussion

In the PVNGS control rooms the SPDS is located next to the Control Room Supervisor's console. The SPDS console is approximately the same height as the operating console so that it does not obscure the Supervisor's visual access to the control boards. An aisle is provided between the SPDS console and the operating console so that it does not interfere with operator movement.

Irrespective of the SPDS's location near the control room supervisor's normal station, the fact that reading control board instrumentation is difficult unless the operator is very close to the displays will tend to draw the supervisor away from the SPDS. This is especially true in light of the relatively slow system update rate that inhibits use of the SPDS in-lieu of the hardwired instrumentation.

4.5.2. LLNL Evaluation

This provision of Supplement 1 to NUREG-0737 will be satisfied by the PVNGS SPDS if the system response time problems discussed in section 4.3 of this report are corrected.

4.6. "THE SPDS SHALL CONTINUOUSLY DISPLAY INFORMATION FROM WHICH THE SAFETY STATUS OF THE PLANT ... CAN BE ASSESSED ..."

4.6.1. Discussion

With the exception of software development and maintenance displays all ERFDADS displays contain CSF Safety Indicator Blocks. A password, not made available to plant operators, is required to display software development and maintenance displays on the control room SPDS console. This software provision ensures the SIBs will be continuously displayed in the control room to provide information from which the safety status can be readily assessed and to alert operators to important changes in safety parameters.

4.6.2. LLNL Evaluation

This requirement of Supplement 1 to NUREG-0737 is satisfied by the PVNGS SPDS.

4.7. "THE SPDS SHALL BE SUITABLY ISOLATED FROM ELECTRICAL OR ELECTRONIC INTERFERENCE WITH EQUIPMENT AND SENSORS THAT ARE IN USE FOR SAFETY SYSTEMS"

4.7.1. Discussion

The PVNGS SPDS design incorporates isolation devices between the SPDS and Class 1-E circuits. These isolation devices are intended to insure that no credible failure of the SPDS will prevent the associated safety related circuit from meeting it's minimum performance criteria. APS has type tested these isolation devices to determine the effect on the isolation device input of short circuits, open circuits, and the application of maximum credible voltage and currents at the output. The methodology and results of this testing are currently under review by the NRC.

4.7.2. LLNL Evaluation

Determination of the acceptability of isolation devices used for the SPDS is not within the scope of this technical evaluation. A judgment concerning APS's compliance with this requirement of Supplement 1 to NUREG-0737 will be the subject of a separate technical evaluation report.

4.8. "PROCEDURES WHICH DESCRIBE THE TIMELY AND CORRECT SAFETY STATUS ASSESSMENT WHEN THE SPDS IS AND IS NOT AVAILABLE WILL BE DEVELOPED BY THE LICENSEE IN PARALLEL WITH THE SPDS. FURTHERMORE, OPERATORS SHOULD BE TRAINED TO RESPOND TO ACCIDENT CONDITIONS BOTH WITH AND WITHOUT THE SPDS AVAILABLE."

4.8.1. Discussion

APS considers the unit Shift Technical Advisor to be the primary SPDS user under plant upset conditions. During a plant transient the STA reports to the Supplemental Technical Support Center adjacent to the unit control room. After reporting to the STSC the STA's duties include monitoring the status of plant safety, and providing advice and assistance to the unit Shift Supervisor. To assess plant safety status, the STA may chose to use either the SPDS display in the STSC, the SPDS display in the control room, or control room hardwired instrumentation.

Unit operators are secondary users of the SPDS. The SPDS is available in the control room to be used by the unit operators as an alternative source of data regarding plant status, and the values and trends of plant parameters.

Operators and STAs have received the same classroom training on the system. This training consisted of an initial class discussing the purpose of the SPDS, the displays available, and how to use the system to assess CSF status. Requalification training has also been conducted. This training included discussion of SPDS development, system modifications, and a demonstration of SPDS operation. Operators and STAs are also required to perform specific on-the-job training (OJT) exercises to complete their qualification on the system. Since the STAs are designated as the primary system users, their OJT program is more extensive. APS does not plan periodic SPDS requalification training for the operators or STAs.

4.8.2. LLNL Evaluation

APS has not completely satisfied this requirement because a control room user of the SPDS, when the STA is unavilable, has not been designated. Although use of the SPDS by the STAs is appropriate and should prove beneficial, the fact that a unit STA is frequently away from the control room disqualifies the STA from being the initial user of the SPDS during the first phase of a transient.

The general outline of operator and STA training appears to be acceptable except that the emphasis has been misdirected away from use by the control room staff. The lack of an APS commitment to periodic requalification training on the use of the SPDS is also of concern because the SPDS is being continually modified. Additionally, need for further requalification training appears to be indicated by the operator comments discussed in Section 3.3.1 of this TER. APS should consider whether requalification training is necessary to maintain proficiency in SPDS use.

To resolve the above concerns APS should identify a control room user for the SPDS. Once this user has been identified, a discussion of revisions made to the training program to account for this change in emphasis should be submitted for NRC review. APS should also review and report to NRC on the need for periodic operator and STA requalification training on SPDS use.

4.9. "THE SPDS DISPLAY SHALL BE DESIGNED TO INCORPORATE ACCEPTED HUMAN FACTORS PRINCIPLES SO THAT THE DISPLAYED INFORMATION CAN BE READILY PERCEIVED AND COMPREHENDED BY SPDS USERS."

4.9.1. Discussion

The PVNGS SPDS design was subject to a two phase APS review against human factors principles. In the first phase the original system design was reviewed against human factors engineering principles derived from NUREG-0700, NUREG-0835, and NUREG-0696 by a team that included a human factors consultant, an instrument and control engineer, and a computer engineer. This review generated a listing of Human Engineering Observations (HEOs). These HEOs were screened to remove items that did not pertain to SPDS functions or that had already been corrected. The HEOs not removed by this screening process became Safety Parameter Observations (SPOs) that were assessed for correction. The SPO assessment process placed each SPO into one of two categories.

Category A	Required to make system meet regulatory requirements.
Category B	Not required to meet regulatory requirements, but correction will be implemented as plant betterment.

After all Category A SPOs had been corrected the human factors review was repeated to verify that all significant human engineering discrepancies had been found and corrected.

Discrepancies identified at this stage were also placed into one of two categories.

Category 1	SPO impacts the SPDS function.
Category 2	SPO does not impact the SPDS function.

The NRC Audit Team reviewed APS plans to correct these SPOs. Although the Audit Team did not agree with the categorization of every SPO, the Team found that in all cases appropriate action on these items has been scheduled by APS.

The NRC Audit Team operated a SPDS terminal being driven by real-time plant data. The Audit Team found the SPDS displays are easily readable, display formats are well laid out and easy to interpret, and data coding is effective and easy to understand. The Audit Team, however, noted a number of minor deviations from accepted human factors practice. These were:

- The mnemonics identifying the CSF associated with each Safety Indicator Block are difficult to read.
- In many cases, color coded text is difficult to read. An example of this on trend plots is the red characters used to indicate the current value of parameters that are in the unsafe range.
- Time units on trend plots do not line up with the corresponding tick marks on the time axis.
- The extraneous word "generation" appears on the log-power trend plot.

The SPDS's control room console keyboard contains a function key for the SPDS overview display and for each of the individual CSF mid-level displays. Alternatively these displays can be accessed through the use of a paging key that sequencially switches the SPDS display through the six CSF displays and the overview display.

When the SPDS is displaying a mid-level display the parameter trend plots can be accessed via use of a paging key that sequentially switches the SPDS display through all trend plots associated with that CSF. Trend plots for the CSF may also be randomly accessed by entering the parameter bar number at the SPDS keyboard.

4.9.2. LLNL Evaluation

The PVNGS SPDS meets the NUREG 0737, Supplement 1 requirement to incorporate human factors principles into the system design. Nevertheless, it is recommended that the NRC Audit Team's findings concerning difficult-to-read SIB mnemonics, and difficult-to-read text be assessed for correction. The placement of scale numbers on the horizontal trend plot axes should be adjusted and extraneous text should be removed from the displays.

The inconsistencies in display conventions from display to display reflect the lack of formal human factors criteria during the display development process. These inconsistencies do not seriously hamper the usability of the user interface. However, APS should develop formal human factors guidance and display conventions in order to avoid incorporating more severe problems into the system when future SPDS modifications are made.

5. SUMMARY

The Palo Verde SPDS fulfills most SPDS requirements of Supplement 1 to NUREG-0737. It is LLNL's opinion, however, that the following items must be resolved in order for the system to completely fulfill these requirements.

- Main steam line radiation must be added to the Radiation Release CSF or acceptable justification provided for not including this parameter in the assessment of this safety function.
- The update rate for deviation bar length and color, and Safety Indicator Block color must be improved. It may also be necessary to improve the update rate and time resolution of trend plots. APS should develop update rate and time resolution acceptance criteria based upon analysis of process dynamics and operator's information needs.
- Interchannel comparison acceptance criteria that are consistent with the expected deviation between valid inputs under both normal and severe environmental conditions must be developed.
- Invalid data should not be used in the determination of CSF status as displayed by the Safety Indicator Blocks.
- The SPDS should be able to ride through the momentary loss of AC power to the DAS, associated with a loss of offsite power, without requiring a lengthy restart cycle for the DAS program.
- A SPDS user who is normally present in the control room should be identified.
- APS should determine if additional and/or periodic retraining on SPDS use is necessary.
- The minor human engineering concerns identified by the NRC Audit Team should be addressed.
- A standard for display formats should be developed to ensure that human engineering problems are not introduced during future system modifications.
- Category 2 validation items and SPO's should be entered into the plant change process for tracking.
- Once the SPDS is operational in the plant simulator, a re-validation of the SPDS should be conducted using simulator scenarios that exercise all Critical Safety Functions, and integrate the use of the SPDS with the EOPs and control board instruments.

APS action on the above items should be described for NRC review to allow a final conclusion regarding the acceptability of the PVNGS SPDS.

GLJ:dm/2/25/87

LLNL also noted a number of items that do not directly affect the acceptability of the SPDS but which, nevertheless, may improve the system's usability. APS should consider addressing the following items as system enhancements.

o Use of the limits of reasonable parameter values, rather than the physical limits of measuring instruments, as range checking criteria would improve this function.

o Revision of trend plot formats so that time progresses from left-to-right instead of right-to-left would remove a potential source of user confusion.

o Indication of current parameter values on second-level displays may improve the usefulness of these displays.

o The parameter trend plots would be more meaningful if the relationship of the current value to the alarm values were displayed. APS should consider alternative methods for showing this relationship in a way that does not clutter the display.

o Addition of Auxiliary Feedwater flow to the Heat Removal CSF displays would provide a early warning that heat removal via the main stream system is in jeopardy. Also, this addition would improve the SPDS user's ability to relate changes in steam generator water level and AFW flow.

LLNL suggests that APS obtain user feedback on the last two items above to determine if the additional information provided on the displays will add to or detract from display usability.

6. REFERENCES

6.1. GENERAL REFERENCES

1. NUREG-0660, "NRC Action Plan Developed as a result of the TMI-2 Accident," Rev. 0, May 1980, Rev. 1, August 1980.

2. NUREG-0737, "Clarification of TMI Action Plan Requirements," November 1980.

3. NUREG-0737, Supplement 1, "Clarification of TMI Action Plan Requirements," December 1982.

4. NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," Section 18.2, "Safety Parameter Display System (SPDS)," Rev. 0, November 1984.

5. "Palo Verde Nuclear Generating Station Safety Parameter Display System Safety Analysis Report," Arizona Public Service Company, February 1985.

6.2. DOCUMENTS EXAMINED DURING AUDIT

6. Departmental Instruction OCSSGLSW01, "Computer Software Maintenance Support Scope and Responsibilities."

7. Procedure, "Review and Approval of Station Procedures," Revision 8.

8. Procedure 73AC-0SPDSSPDS27, "Change Control Process," Revision 3.

9. Specification 13-JN-106A, "Technical Requirements for the Arizona Public Service Safety Parameter Display System Bar Driver Algorithms," Revision 4, July 25, 1986.

10. Specification 14273-ICE-3057, "General Specification for the Software Design of the Qualified Safety Parameter Display System for Arizona Public Service Company, Palo Verde Nuclear Generating Station," Revision 00, February 3, 1983.

11. Program Listing, "ITL Program SAP," Revision 29.

12. Report, CE-NPSD-239, "Accident Monitoring Instrumentation Accuracy Evaluation," no date.

13. Procedure, APS-8-916, "Emergency Response Facility Data Acquisition and Display System Site Demonstration Test."

14. Test Results Report, 92CM-1SD01, "ERFDADS Isolation Cabinet Power Supplies Test Report."

15. Test Results Report, 92GT0SPDSPDS04, "Instrumentation and Control Loop Functional Verification."

ENCLOSURE 2
PEICSB SALP INPUT

Plant: Palo Verde Units 1, 2, and 3
Licensee: Arizona Public Service Company
Docket No. 50-528, 50-529, and 50-530
SER Subject: Safety Parameter Display System

PERFORMANCE PARAMETERS:

(1) Management Involvement in Assuring Quality

(2) Approach to Resolution of Technical Issues from a Safety Standpoint

(3) Response to NRC Initiatives

(4) Staffing (Including Management)

(5) Reporting and~Analysis of Reportable Events

(6) Training and Qualification Effectiveness

(7) Any other SALP Functional Area

PERFORMANCE PARAMETER	NARRATIVE DESCRIPTION OF LICENSEE'S PERFORMANCE	CATEGORY/RATING
(1)	The licensee's management is committed to a useful SPDS. A program to correct deficiencies and update the SPDS is actively supported.	2
(2)	The licensee's staff did provide an adequate response to staff concerns on isolation devices.	2
(3)	Not Applicable	
(4)	Not Applicable	
(5)	Not Applicable	
(6)	Not Applicable	
(7)	Not Applicable	

Overall Rating: Category 2