PALO VERDE

TECHNICAL AUDIT

November, 1984

TABLE OF CONTENTS

1.0 Executive Summary

A review of technical documents prepared for Palo Verde by Combustion Engineering (C-E) found inconsistencies in component response times. The inconsistencies were small in number, inconsequential to safety, and rectified by revising the draft Technical Specifications. However concern was raised that a more general problem might exist. C-E therefore performed a complete review of all response times, and elected to conduct a separate independent technical audit of design activities associated with Palo Verde.

The technical audit was structured to cover a broad range of technical activities and organizational interfaces, and was conducted by senior engineering personnel not previously associated with the activities audited. The audit took place during October and November, 1984. It required approximately 3300 manhours, and approximately fifteen percent of the SAR safety analysis parameters were audited.

The audit found no serious technical errors, no safety concerns, and no systematic error patterns. The design process was found to be adequate and conservative.

2.0 Introduction

Proposed Technical Specifications are normally prepared in conjunction with a Final Safety Analysis Report (FSAR). During the subsequent review period, revisions may be made to both documents, creating a potential for inconsistent use of data. At the request of Arizona Public Service (APS) Company, Combustion Engineering conducted a review in August and September of 1984 to confirm consistency among the latest draft of the Palo Verde Technical Specifications, the Palo Verde FSAR, and CESSAR-F.

C-E's review (and an NRC review which occurred in the same period), found several inconsistencies in component response times. Specifically, the response times allowed for certain Reactor Protection System (RPS) and Engineered Safety Feature (ESF) components in the technical specifications were not conservatively bounded by the CESSAR-F safety analyses. On October 4, 1984, representatives of C-E, Bechtel, and Arizona Public Service met with the NRC to discuss the cause of each error and the corrective actions to be taken. In each case, the error resulted from a miscommunication between C-E's safety analysis groups (responsible for FSAR analyses) and C-E's design groups (responsible for setting technical specification limits). The errors were of inconsequential safety significance and were rectified by revising the technical specification limits to match the assumptions of the safety analyses.

To assure that the errors were isolated instances, C-E reviewed RPS and ESF response times for all of the CESSAR-F and Palo Verde safety analyses. Although this review was considered by C-E to be sufficient to close the issue for the Palo Verde Operating License, C-E also considered it prudent to conduct an independent audit of the Palo Verde safety analyses (and applicable CESSAR-F analyses) to check for consistency with C-E design specifications, interface requirements, technical specifications and reasonable engineering judgment, and to determine if any detected inconsistencies might be indicative of a more general but as yet undetected problem. The program and the results of the audit are described in this report.

3.0 Description of Audit

3.1 Purpose

The Technical Audit was specifically structured to examine certain aspects of the NSSS design process at Combustion Engineering as applied to Palo Verde. The previously discovered inconsistencies, although not significant to the safety or the performance of the nuclear unit, were of concern. The audit was designed to include a determination of the presence or absence of systematic error patterns in the design process. A secondary objective was to develop information which could be used to improve the efficacy of the design process if the need for improvement was found.

3.2 Personnel

The Technical Audit was carried out by a team of independent senior technical personnel who were responsible for planning and performing the audit activities.

Responsibility for the audit was assigned to Systems Engineering, a special unit of the Nuclear Power Systems Engineering Department. Systems Engineering does not have line responsibility for NSSS design activities, and consists of senior technical personnel and special service groups. The Director of Systems Engineering was the Audit Team Leader, reporting to both the Vice President, Engineering and the Vice President, Commercial for purposes of this audit.

The auditors were chosen for technical competence, prior experience with the C-E NSSS design process, and diversity in technical specialties. All of them have current positions equivalent to that of a supervisor or manager in the engineering organization. Five are currently assigned to Systems Engineering, one to Nuclear Engineering. Each has an advanced degree in engineering or science, and is currently assigned to projects not directly associated with current NSSS design projects. Each audited areas in which he had no previous involvement as a designer, independent reviewer, or manager.

3.3 Scope and Target Selection

The entire Audit Team participated in the planning of the audit activities. Planning was carried out during the first week of the audit period.

The first goal of the planning process was the selection of a method of identifying meaningful target areas. The need to cover a broad range of activities and organizational units, and the desired emphasis on communication and possible systematic errors, led to a novel approach.

Starting with the Palo Verde FSAR, twelve events were selected from Chapters 6 and 15 which covered the range of activities desired. Then, thirteen important parameters of the design process were chosen which were (1) well distributed in the selected events, (2) included all important safety functions, and (3) had a high probability of involving meaningful audit areas. The twelve events and the thirteen parameters were arranged in a matrix, so that the appearance of a parameter in the analysis of an event could be identified at an intersection on the matrix. The intersections were examined as potential audit areas, and a final matrix was adopted following minor adjustments. Care was taken to insure that one event (Steam Generator Tube Rupture) included all parameters. Likewise, one parameter (Moderator Temperature Coefficient) appeared in all events.

One auditor was assigned exclusively to the full range event, and another to the full range parameter. The other intersections of the matrix were assigned to other auditors, using the parameters as the audited feature.

The final matrix is shown as Figure 1. The audited intersections are identified with Roman numerals, which also serve as a key to the Summary of Findings (Section 4) for that intersection. Also shown on Figure 1 is whether each event is limiting (L) or non-limiting (NL), Palo Verde specific (PV) or CESSAR (C). (One of the second order event selection criteria was to provide a reasonable distribution in each of these categories.)

In total, there are 64 intersections, or targeted audit areas, of which thirteen (the steam generator tube rupture event) received the attention of two auditors from different perspectives. Thus, the audit covered a total of 77 audit areas.

To provide some appreciation for the size of the sample, CESSAR contains some 37 events (discarding similar cases such as a series of LOCA analyses with differing break sizes), with an average of about ten reported parameters per event, yielding 370 intersections. Of the 64 intersections in this audit, about 55 fall in the same category. Therefore, approximately 15% (55 out of 370) of the CESSAR intersections were audited.

The audit took place over a period of five weeks. During that time, the auditors and the designated contacts in the audited organizations (whose contribution often exceeded the auditor's) spent approximately 3300 engineering manhours, not including supervision and non-technical support.

The audit encompassed engineering activities that 1) occurred over a time period of more than a decade (approximately 1973 to 1984), 2) was effected by changing regulatory requirements (e.g. 10 CFR 50, Appendix B changes), and 3) was subject to changing staff assignments. Consequently, the audit was also an examination of C-E's approach for continuity of information exchange, documentation adequacy, and technical management.

3.4 Audit Procedures and Groundrules

In addition to the development of the matrix scheme for identifying target areas, the Audit Team established the procedures and groundrules for conducting the audit. These were reviewed and approved by management, and were then presented, in concert with the target areas, in a pre-audit meeting held with the audited organizations. The major groundrules were:

- Each audited group is to provide competent technical assistance to the auditor. The assistance includes providing a "flow chart" of the design process associated with the audited parameter, pertinent documention, and access to other technical personnel as necessary.

- The auditor is, by definition, not previously associated with the audited area. If he finds himself in a conflict-of-interest situation, he asks another auditor to perform that portion of his audit activities.

- The auditor may choose to audit in varying depth the numerous paths that may appear during his investigation. Generally speaking, he should concentrate on the more complex relationships because simple paths through the design process are less likely to contain errors.

- Because none of the selected events or parameters originates in the Instrumentation and Control Engineering area, interfaces into and out of I&CE should be given special attention to insure a balance in auditing activity.

- The audit is not intended to determine compliance with formal quality assurance procedures. Problems in this area should be noted, but the auditing is to concentrate on the technical aspects of the design process.

- Inconsistencies discovered during previous review activities are excluded from the scope of this audit to avoid duplication of effort. If they are encountered, the occurrence should be noted, and the auditing should proceed to other areas.

- The auditor's job is to examine the record, not change it. If problems are found, normal corrective procedures can be followed by the originating organization.

- Maximum use should be made of existing auditing material and information. For example, the technical portions of check lists used for formal QA procedures are useful in evaluating the use and transmittal of technical data.

As a result of the pre-audit meeting, each major group of the engineering organization volunteered to assign one or more technical representatives to assist the auditors, prepare the flow charts, arrange for the retrieval of pertinent documentation, and establish other technical contacts within the department as necessary. This greatly facilitated the audit activities, and the entire process was carried out smoothly and efficiently.

The Audit Team met regularly throughout the audit period to compare notes, exchange views, discuss problems and solutions, avoid overlapping efforts, and monitor progress.

Management was periodically briefed on the activity as it progressed.

4.0 Summary of Findings

This section summarizes the findings of the audit of each matrix intersection. Summary findings are presented for each parameter audited and for the audit of the steam generator tube rupture event analysis.

Moderator Temperature Coefficient (I, II, III)

This portion of the audit examined the analytical prediction of reactivity addition due to moderator temperature change and its use in the safety analyses. All events shown in Figure 1 were reviewed relative to the use of the MTC. The review was separated into three parts: overcooling events analyses, loss-of-coolant accident analyses (LOCA), and all other events noted in Figure 1.

The overcooling events included increased main steam flow and main steam line break. The main steam line break analyses are used to set the lower (negative) limit for the MTC used in the Technical Specifications. It was found that the value of MTC calculated for cooldown following reactor trip was accomplished with considerable conservatism and that the data was used consistently and accurately throughout the analyses.

The LOCA analyses are used to set the upper (positive) limit for the MTC used in the Technical Specification. The development of MTC data for LOCA analyses is done independently from that for other analyses and is treated as a density coefficient to allow for voiding in the moderator. The moderator temperature coefficient of 0.0×10^{-4} /°F at normal operating conditions was used in the limiting small break analysis and development of the Technical Specifications.

For all other events, the audit showed that the MTC data generated by Nuclear Engineering was used in several different areas and required additional handling and manipulation of the data. Three events in CESSAR were identified where the data reported to have been used differed from that actually used in the analysis. However, in none of these cases was MTC a critical parameter. It appears that the discrepancies occurred during the handling and manipulation required for a specific use of the data. The specific events with discrepancies are the steam generator tube rupture, CEA drop, and CEA withdrawal. There appears to be significant conservatism in both the calculation and the application of the MTC data; as a result, the analyst has some degree of latitude in the selection of specific MTC input for a given event while still maintaining a conservative result. In particular, for the three events listed above the overall results are considered to be conservative.

Steam Generator Tube Rupture Event Analysis (IV)

This audit activity differed from the others in this audit; it focused on an event rather than a group of parameters. Otherwise the audit procedures were the same.

The audit consisted of two parts. The first part was a review of the steam generator tube rupture event and related input parameters. The audit purposes were to determine if: 1) input parameters were employed in an appropriate and internally consistent manner in the event, and 2) appropriate interfacing among functional groups occurred.

The second part of the audit was an investigation of how the narrow range safety injection tank water level instrumentation that is used to monitor a technical specification parameter was treated by the groups involved in establishing design requirements, equipment specifications, technical specifications, and performing related safety analyses. The specific instrument channel was selected as a representative example of non-1E, non-post-accident instrumentation.

It was determined that:

1. Input parameters were used appropriately and in a manner consistent with their impact on the consequences of the steam generator tube rupture event. Reasonable engineering judgments were made in deciding how to use and/or modify input parameters.

2. Generation of input parameters was consistent with the intended use and was based on information contained in related documents such as interface requirements, technical specifications, and equipment specifications.

3. Information exchange and interfacing within C-E NPS Engineering and among C-E, Bechtel, and the Arizona Nuclear Power Project was adequate.

4. No systematic design process deficiencies were evident. Some minor discrepancies were observed but were of no technical importance. Such discrepancies were, in general, known to the cognizant engineers and had been previously judged to be of no significant consequence. (The parameter discrepancies encountered are addressed fully in the Summary of Findings for that parameter.)

5. Technical Specifications encountered in the audit were consistent with audited parameters and other related data, excluding those inconsistencies already found as a result of previous studies performed for Palo Verde.

6. There are specific programs to review instrumentation that is associated with either a safety system (1E) or post-accident monitoring. No routine program exists for non-1E, non-post-accident instruments (such as the safety injection tank narrow range water level) used to maintain technical specification limits. However, the audit found a consistent treatment among setpoints, technical specifications, and operational requirements for the SIT narrow range water level instrumentation.

CEA Worth at Scram (V)

This activity was a review of the bases for developing the CEA worth at scram and to determine if this parameter was used with consistency in the safety analyses. The CEA worth at scram was appropriately used and consistent with the design documentation and Technical Specifications reviewed. The interfacing organizations added conservatism to this design parameter prior to using it. It was observed that the CEA worth given in Table 15.4.1-4 of the FSAR was not consistent with the design documentation. The analysis (Rod Withdrawal Event) used -6.4% and not the -3.6% noted in the table. The analysis value of -6.4% is the appropriate value.

Core Mass Flow (VI)

This portion of the audit was a review to determine if the core mass flow was used with consistency in the design process and if related inputs to interfacing organizations supported the original design bases. It was determined that the core mass flow was used appropriately and that engineering information transmitted to interfacing organizations was consistent with design requirements.

HPSI, LPSI Lag Times (VII)

This portion of the audit examined the consistency in the definition, value, and use of safety injection pump lag times. It was determined that the lag times were consistently defined as the total elapsed time from the receipt of the safety injection actuation signal to the time the pumped safety injection water enters the reactor coolant system. Most analyses used 30 seconds as the lag time. Some analyses used a lag time that was conservative relative to 30 seconds.

Initial Pressurizer Level (VIII)

The scope of this audit activity was to verify if the initial pressurizer level utilized in the safety analyses was properly established by the design process. Selected pressurizer level control parameters were examined to verify that pressurizer level could be maintained within the "Limiting Condition of Operation" specified in the Technical Specifications. The initial pressurizer levels used in the safety analysis were chosen conservatively, and the pressurizer level "Limiting Conditions of Operation" specified in the Technical Specifications were conservatively established relative to the pressurizer levels chosen for use in the

subject safety analyses. The engineering data inputs to establish the pressurizer level control program were properly executed at each interface in the design process. Pressurizer level control parameters were properly described in control system equipment specifications, and control system setpoints were properly transmitted.

Initial Steam Generator Level (IX)

This audit activity examined how the initial steam generator level utilized in the safety analyses was established and communicated by the design process. The bases for the volumetric and liquid mass parameters specified for the respective initial conditions of the safety events were identified in several data transmittals.

It was determined that:

1. The selection of the initial steam generator liquid inventories was consistent with accepted practice and/or methodology.

2. The liquid mass parameters calculated for input to the Main Steam Line Break accident were properly adjusted to account for thermal and internal pressure expansion of the steam generators.

3. The liquid mass parameters used as input to the Chapter 15 safety analyses were properly correlated to the initial liquid level assumption specified for the subject event.

Condensate Storage Tank Capacity (X)

This audit activity examined the initial bases for establishing the size of the condensate storage tank and the verification of selected engineering inputs to the analysis. Verification of the analysis methodology was reviewed by utilizing the natural circulation test results from a C-E operating plant. The Chapter 15 events were reviewed to verify that adequate condensate capacity was specified to accommodate these transients, and to assure that the atmospheric dump valve capacity, installed at Palo Verde is consistent with the analysis assumptions.

It was determined that:

1. The condensate storage tank capacity is more than adequate to accommodate a natural circulation cooldown for all the Chapter 15 events that were audited.

2. Engineering verification trails were evident and special attention had been given to verification of the atmospheric dump valve capacity prior to initiating the Chapter 15 analyses.

3. Technical Specifications properly define the condensate storage capacity requirements.

Valve Closure Times (XI)

This part of the audit examined the use of the closure times for the following valves: Main Steam Isolation Valve, Shutdown Cooling System Isolation Valve, and Letdown Isolation Valve. No inconsistencies were found beyond those previously discovered during the Palo Verde Technical Specification consistency check.

HPSI, LPSI Flow Rates (XII)

This audit activity was a review of the calculations documenting the methods for computing HPSI and LPSI flow rates and the process by which these results were transmitted and used in the safety analyses. This was done to determine the basis for defining the curves for safety injection flow versus RCS pressure and to check for consistency in the use of these curves in the safety analyses.

An inconsistency was found in the use of HPSI flow rates. This inconsistency was judged to have a minor effect on the results of the affected analyses and consequently is of no safety significance. The inconsistency is explained below.

The initial values of safety injection flows were based on preliminary safety injection pump performance curves and calculation of flow versus head values. The initial set of curves were used in the analyses of increased main steam flow, steam generator tube rupture, and large and small break LOCA's events. HPSI pump test data was used to calculate a modified set of flow versus pressure curves. The new curves resulted in slightly higher flows (about 10%) at pressures above 600 psig and lower flows (about 1%) at pressures below 600 psig. The revised flows were used in the small break LOCA analysis. The difference in flow was judged to have a minor effect on the results of the steam generator tube rupture event, and therefore the original flows were used. The flow change had no impact on the increased main steam flow events (i.e. inadvertent opening of a steam generator atmospheric dump valve) because HPSI pumps were not actuated during the transient. The original flows were also used in the large break LOCA analysis since this is conservative.

Containment Spray System Parameters (XIII)

This audit activity was a review of the process and documentation defining, transmitting, and using containment spray system parameters in the safety analyses. The objective was to verify the consistency in transmittal and use of two of the parameters related to the design and performance of the Containment Spray system; net positive suction head (NPSH) and design flow rate. It was determined that the parameters were used consistently and/or conservatively throughout the work.

CEA Scram Time (XIV)

This part of the audit reviewed the use of CEA scram time in the safety analyses and its development through the design process. A few parameter inconsistencies were found. None were determined to be of safety significance. The inconsistencies are described below. The events involved were the loss of condenser vacuum, steam generator tube rupture, single CEA drop, and small break LOCA. All other events examined used information that was consistent with the design documentation.

1. In the loss of condenser vacuum and steam generator tube events some inconsistencies were noted relative to the definition of trip actuation response times and rod insertion times in developing total elapsed time for CEA SCRAM. However, these individual inconsistencies had no effect on the total elapsed time or the results of the analyses.

2. The single full length CEA drop event was also reviewed to compare the scram time used for consistency with other events. This comparison was made because the events identified in the matrix are bounded by reactivity concerns or the maximum allowable scram time; while it is the fastest CEA drop time that should become the input for the CEA drop analysis. The fastest CEA drop time was not identified for input into the CEA drop analysis; however, a drop time of 2 seconds was chosen. A review of the CEA scram analysis, conducted during the audit, showed that 2 seconds was conservative.

3. The small break LOCA analyses used the 4 seconds scram time associated with the normal operating conditions for CEA insertion; however, the thermal hydraulic conditions associated with the small break LOCA were not considered in the evaluation of CEA scram time. Engineering evaluated this discrepancy and determined that the design conditions envelope the thermal hydraulic conditions associated with the small break LOCA during the time of CEA insertion.

Diesel Generator Start Time (XV)

This part of the audit examined the use of the diesel generator starting time value used in the safety analysis. No inconsistencies were found in the application of this parameter.

Reactor Coolant Activity (XVI)

The audit activity examined if a consistent and/or conservative values of reactor coolant activity were used in the safety analyses. The examination showed that both consistency and conservatism were present in the use of this parameter.

5.0 Conclusions

The audit confirmed the adequacy of C-E's NSSS design process. The auditors determined that there are:

- o No systematic error patterns in the design process used for Palo Verde.
- o No serious technical errors and no safety concerns about the engineering done for Palo Verde.

The C-E design process is adequately sensitive in areas important to nuclear safety and power plant performance, and sufficiently conservative to accommodate occasional random errors. The process is also capable of effectively carrying out large projects involving extremely complex relationships, over long periods of time, with changing personnel and requirements.

The few inconsistencies found in the audit either were of a documentation nature in which the analyses used more appropriate values than those reported, or involved parameters that did not have a significant impact on safety consequences of specific analyses. In both cases it appears that a conscious decision was made by the cognizant engineer to focus attention on the more significant aspects of the analyses and proceed with the work as it was finally observed by the auditors. Consequently, it can be concluded that reasonable and conservative engineering judgment was applied in the Palo Verde design process.

EVENTS

PARAMETER	15.1.3 INCREASE MAIN STEAM FLOW	15.2.3 LOSS OF CONDENSER VCM	15.2.4 MSIV CLOSURE	15.2.7 LOSS OF FEEDWATER	15.3.4 RCP SHEARED SHAFT	15.4.1 ROD WITHDRAWL	15.4.3 ROD DROP	15.4.6 INADVERTENT DILUTION	15.5.2 CVCS MALFUNCTION	15.6.3.2 S/G TUBE RUPTURE	CHAP 6 MSLB	CHAP 6 LOCA
	NL	L	NL	NL	L	NL	L	NL	L	L	NL	NL
	C	PV	C	C	PV	C	C	C	C	PV	PV	PV
MODERATOR TEMP COEFF	I	II	II	II	II	II	II	II	II	II & IV	I	III
CEA WORTH AT SCRAM	V				V	V		V		V & IV		
CORE MASS FLOW RATE			VI		VI	VI	VI			VI & IV		
LAG TIMES FOR HPSI & LPSI PUMPS	VII									VII & IV		VII
INIT PRESSURIZER LIQUID LEVEL		VIII	VIII			VIII	VIII		VIII	VIII & IV		
INIT S/G WATER LEVEL	IX	IX	IX	IX						IX & IV	II	
CONDENSATE STORAGE TANK CAPACITY		X		X	X				X	X & IV		
CONT. ISO VALVE (MSIV,SCCS,LETDOWN) CLOSURE TIMES	XI									XI & IV	XI	XI
HPSI & LPSI FLOW RATES	XII							XII		XII & IV		XII
CONT. COOLING SYS (FAN COOLERS/SPRAYS)										XIII & IV	XIII	XIII
CEA SCRAM TIME		XIV	XIV	XIV						XIV & IV		
DIESEL-GENERATOR START TIMES					IV				IV	IV & IV		IV
INITIAL RCS ACTIVITY										XVI & IV	XVI **	XVI

L - LIMITING EVENT NL - NON-LIMITING EVENT PV - PALO VERDE SPECIFIC C - CESSAR GENERIC

** - THE MSLB, AS PRESENTED IN SECTION 15.1.5. WAS REVIEWED FOR THE INITIAL RCS ACTIVITY IN LIEU OF THE CHAPTER 6 PRESENTATION

FIGURE 1