JAN 2 9 1991

Mr. William H. Rasin
Director, Technical Division
Nuclear Management and Resources Council
Suite 300
1776 Eye Street, N.W.
Washington, DC 20006-2496

Dear Mr. Rasin:

Enclosed for your information is an advance copy of NUREG-1397, "An Assessment of Design Control Practices and Design Reconstitution Programs in the Nuclear Power Industry." This NUREG, which will be published shortly, provides NRC observations regarding current utility design control practices and design reconstitution programs.

Sincerely,

Original signed by

William T. Russell, Associate Director
for Inspection and Technical Assessment
Office of Nuclear Reactor Regulation

Enclosure: As Stated

Distribution: w/o enclosure
WTRussell, NRR
TEMurley, NRR
FJMiraglia, NRR
BKGrimes, NRR
WDLanning, NRR
EVImbro, NRR
RAGramm, NRR
WHBateman, EDO
PDR
Central Files
DRIS R/F
RSIB R/F

9102060205 910129
PDR ORG NRRB
PDR

*See previous concurrence

SC:RSIB:DRIS	C:RSIB:DRIS	D:DRIS	AD:NRR
EVImbro*:sf	WDLanning*	BKGrimes	WTRussell
01/29/91	01/29/91	01/29/91	01/ /91

050031

ENCLOSURE

NUREG-1397

An Assessment of Design Control Practices and Design Reconstitution Programs in the Nuclear Power Industry

U.S. Nuclear Regulatory Commission

Office of Nuclear Reactor Regulation

E. V. Imbro

ABSTRACT

This document summarizes the results of a survey of nuclear power plant design control practices and design reconstitution efforts conducted during 1989 at six utilities and with one nuclear steam supply vendor. Conclusions and observations resulting from the survey assessments are provided so that utilities and the NRC can consider actions to improve these programs.

CONTENTS

CONTENTS (Continued)

CONTENTS (Continued)

EXECUTIVE SUMMARY

The U.S. Nuclear Regulatory Commission (NRC) and the utilities have identified shortcomings involving the maintenance of well-defined design bases and the availability of the necessary supporting design documentation. Many utilities have embarked on design-document reconstitution programs although there has been no clear consensus regarding what information should be included in design-bases documents, what is the minimum set of necessary design documents to support the design bases, or how missing or deficient design documentation should be handled.

The NRC initiated a survey to ascertain the status of design control programs within the industry and the approaches to design-bases documentation used by some utilities. The survey scope included six utilities and one nuclear steam supply system vendor. Observations and conclusions presented by the survey team in no way reflect NRC requirements. Subsequent to this survey, industry guidance entitled "Design Basis Program Guidelines" was published by the Nuclear Management and Resources Council (NUMARC 90-12). As stated in a letter from W. T. Russell to W. H. Rasin dated November 9, 1990, NUMARC's approach will provide a useful approach and worthwhile insights to those utilities undertaking design basis programs of various scopes. The letter also transmitted NRC perspectives on several areas not extensively addressed by the NUMARC guidelines which are consistent with the perspectives contained in this report.

While utilities with large design organizations (typically associated with units that have been recently licensed) feel that a review of the design bases and creation of design-bases documents (DBDs) is not necessary, there are several factors that bear on the need to develop DBDs. Such factors include the eventual loss of design personnel with long-term system design knowledge and the evolution of the utility from a design to an operating environment.

Since each utility has different needs and functions that will be satisfied by the DBDs, an assessment directed to the intended use of the DBDs and a determination of who the primary users will be can provide information to structure the format and content of the DBDs. A centralized location for design-bases information that emphasizes the design intent and an index to design documents that reflect the current plant configuration are key features of successful design-document reconstitution programs. Having this information in a user-friendly format that is readily accessible can enhance design control and configuration management. While it is expected that most DBDs will contain certain similar types of information, the format and content of DBDs will of necessity be somewhat different for each utility.

Strong design-document reconstitution programs are characterized by extensive involvement of utilities in the development of their design-bases documents, including dedicating utility personnel to perform some elements of the design-bases document preparation. Increased utility involvement can enhance the quality of the design-bases documents, lead to greater acceptance and understanding of the design-bases documents by utility personnel, and increase utility personnel knowledge about the aspects of plant design.

Reestablishment of the design bases without reconstitution of the supporting design documents may not provide a sufficient level of information to support future modifications and current plant operation. One important outcome of a design-document reconstitution (DDR) program is continuity among the various levels of design information (e.g., design calculations and design-bases documents) and the physical plant characteristics. A strong DDR program can ensure that the design-bases documents accurately reflect the source design documentation, the design output documents accurately reflect the design bases, and the plant configuration is in accordance with the design output documents.

When plant modifications are made, there must be confidence that sufficient design documentation is available to verify the implementation of the design bases and to provide justification that key design parameters (e.g., pump net positive suction head) are adequately accounted for in the design to ensure that a structure, system, or component will perform its intended safety function. Establishing this confidence is an integral part of the DDR process. The use of a template to identify design documentation necessary to demonstrate the implementation of engineering design-bases before beginning a system or topical design-bases document is a good approach. It can define the design attributes and parameters necessary to demonstrate that structures, systems, and components will perform their intended function. The use of a template will assist in identifying areas where there is missing design documentation. Only one of the utilities surveyed had used a template to systematically identify the system functions and design bases for which they should have design documentation.

Most utilities surveyed had not included a technical review of the supporting design calculations and analyses in their DDR programs and had not defined the set of design documents or design parameters that are necessary to ensure that safety-related structures, systems, and components will perform their intended safety function. A review of each design document retrieved can verify that it is technically sound and consistent with the as-built facility. When missing or deficient design documents are identified, a predefined prioritization methodology can ensure that resources are focused on regenerating these design documents, if necessary, or reconciling document deficiencies or discrepancies on a time scale commensurate with the perceived safety significance of the deficiencies or discrepancies. An initial screening process is useful in quickly determining the safety significance of a missing design document and the effect on plant operability and reportability requirements.

It is likely that the implementation of a DDR program will reveal that certain design documents will be unretrievable or contain inconsistencies. While the regeneration of the complete set of design documents may not be necessary, it is important that certain design documents are available to support plant operation. This set of design documents, referred to as "essential design documents," must be accurate and those that are unretrievable or deficient need to be regenerated or reconciled. In the view of the survey team, essential design documents are (1) those necessary to support or demonstrate the conservatism of technical specification values such as pump flow calculations and set point calculations and (2) those necessary both for use by engineering personnel to support plant operations and for use by the operators to quickly respond to events. Examples of essential design documents include, but are not limited to, electrical load lists, set point lists, valve lists, instrument lists, fuse lists, breaker lists, Q-lists, diesel generator load sequencing, P&IDs, flow diagrams, electrical single-line diagrams and schematics, and breaker and fuse coordination studies.

The regeneration of missing or inaccurate essential documents should be given a high priority. However, if a high level of confidence can be established in the ability of the system to fulfill its safety functions through alternate means, such as test data, it may be possible to give a lower priority to the regeneration of the essential document.

Other than the essential documents discussed above, it may not be necessary to regenerate missing design documents if other supporting information or test data is available to demonstrate that a system, structure, or component can perform its intended safety function. For example, it may not be necessary to regenerate all missing piping support calculations if, on the basis of reanalysis of a sufficient sample, it can be demonstrated that adequate design margins exist. However, if a modification is proposed that would affect a piping support, good engineeering practice would dictate that it be reanalyzed unless a valid analysis exists establishing the point of departure for the proposed modification. Additional analyses can be performed to demonstrate that an adequate design margin exists following the implementation of the modification.

The programs to implement design changes were generally thorough at the six utilities surveyed. However, some of these utilities did not have a formal procedure to define the process for approving a modified item for operation and some did not have a procedure requiring walkdowns of a modification before and after it was implemented.

The conclusions and observations of the survey team resulting from the assessments conducted are provided so that utilities and the NRC can consider actions to improve these programs.

PREFACE

This report is being issued to provide the results of a survey reflecting the scope and performance of several utility design-change control programs and design-document reconstitution programs. Observations and conclusions contained in this NUREG reflect the opinions of the survey team and do not constitute NRC requirements. The reader is also referred to "Design Basis Program Guidelines" contemporaneously being issued by the Nuclear Management and Resources Council for related industry guidance.

ACKNOWLEDGEMENTS

A number of individuals made important contributions to the development of the scope of this report, the collection of information from industry, and the preparation of the report. Dr. Andres DuBouchet provided valuable insights and advice in the area of piping and structural analysis, Mr. James M. Leivo in the areas of instrumentation and control and electrical power distribution systems, and Mr. David Waters in the areas of mechanical systems design, nuclear licensing, and plant operations. Mr. Waters also integrated the input from the other team members and was largely responsible for developing the first draft of this report.

Mr. Brian Grimes, Director of the Division of Reactor Inspection and Safeguards, provided valuable guidance in developing the scope and direction of the survey and this report. Mr. Robert Gramm of the NRC staff provided valuable assistance and suggestions preparing the final report. This report was edited by Ms. Dee Gable who contributed her considerable talents to ensure the report is coherently and logically organized and readable.

The insights gained in this survey would not have been possible without the cooperation of the utilities and the NSSS vendor that graciously consented to participate. These are listed below.

Carolina Power and Light
Pennsylvania Power and Light
Pacific Gas and Electric
Florida Power Corporation
Omaha Public Power District
Florida Power and Light
General Electric Company

The survey team also wishes to thank the Florida Power Corporation for permitting us to include examples of shutdown logic diagrams, safety function diagrams, and system logic trees that were prepared as part of its configuration management program. These have been included as Appendix E to this report.

ABBREVIATIONS

ABD	analysis-based document
AFW	auxiliary feedwater
ANSI	American National Standards Institute
ASME	American Society of Mechanical Engineers
A/E	architect/engineer
CFR	Code of Federal Regulations
CMIS	configuration management information system
DBD	design-bases document
DDR	design-document reconstitution
EFW	emergency feedwater
FSAR	final safety analysis report
HPCI	high-pressure coolant injection
IEEE	Institute of Electrical and Electronics Engineers
LER	licensee event report
NRC	Nuclear Regulatory Commission
NSAC	Nuclear Safety Analysis Center
NSSS	nuclear steam supply system
NUMARC	Nuclear Management Resources Council
PRG	plant review group
P&ID	piping and instrumentation diagram
RHR	residual heat removal
SSC	structure(s), system(s), and component(s)
SSFI	safety system functional inspection
SSOMI	safety system outage modification inspection
USAR	updated safety analysis report

1 INTRODUCTION

1.1 Background

A combination of factors have contributed to the need for utilities to investigate the adequacy and completeness of the set of design bases, design analyses, and final design output documents that define the design of their plants. A consistent finding of Nuclear Regulatory Commission (NRC) inspections (particularly safety system functional inspections [SSFIs] and safety system outage modification inspections [SSOMIs]) is that utilities have not adequately maintained well-defined design bases, nor have they maintained adequate supporting design analyses or final design output documents. This has resulted in plant modifications that have been made without a firm understanding of the available design margins and how they have been affected by the modification. Some of the findings from NRC inspections that have demonstrated inadequate engineering design bases are discussed below.

- During an SSFI at Turkey Point in late 1985, the NRC staff found that the design-bases assumption of auxiliary feedwater (AFW) system functionality on the loss of the non-safety-related instrument air supply to the AFW flow control valves had not been verified by test. Subsequent testing showed that the safety-related nitrogen system, which provides backup to the instrument air supply, had sufficient capacity for 6 to 7 minutes rather than the assumed 15 to 20 minutes that formed the basis for related operating procedures and training. Therefore, the operators were under the impression that they had more time to supply additional nitrogen. Additionally, it was found that the set point of the low-pressure nitrogen annunciator had been reduced from 1000 psig to 500 psig without an adequate safety evaluation; a design-bases requirement to ensure sufficient AFW flow to each steam generator after a dual unit trip had not been incorporated into the emergency operating procedures; and the design bases and supporting analyses were not readily available.

- During an SSFI at Pilgrim in late 1985, the NRC staff found that the design bases and design criteria for the high-pressure coolant injection (HPCI) system existed in various controlled and uncontrolled documents that were not easily retrievable. The lack of a HPCI system description resulted in numerous inaccuracies in the HPCI operator training materials. The lack of traceability to the design bases led to problems in establishing some instrument set points and assuring proper equipment sizing.

- During a SSOMI at Fort Calhoun also in late 1985, the NRC staff identified the failure of the utility to obtain, maintain, and use design-bases information to ensure that original design margins were not violated. For example, the utility had disconnected 2 cells from the 60-cell safety-related battery to reduce the maximum voltage on the dc system during battery charging. However, the adequacy of the 58-cell battery capacity was based on a load profile developed in 1979 that had not been updated to account for new loads added to the dc bus. In addition, the load table used to construct the discharge profile was composed of general loads without supporting references to substantiate detailed loads. Since the original design bases and associated calculations had not been maintained in a workable form, the updated safety analysis report (USAR) was heavily relied on as a design input source document. While the USAR contains design-bases information, it is a licensing document and does not contain all the information needed by the engineer designing a modification. The information contained in the USAR also can be as much as 18 months behind the current plant configuration.

- During an SSFI at Arkansas Nuclear One in early 1986, the NRC staff identified that a single failure of an active component in the vital power supply in conjunction with a steamline break could have resulted in a simultaneous blowdown of both steam generators. The failure of one vital power supply would have caused both steam generators to be cross-connected through the turbine-driven emergency feedwater (EFW) pump's steam supply line, resulting in a loss of EFW flow to both steam generators. The NRC approved the design with the specification that check valves would be used to prevent such a scenario. However, the utility eliminated these check valves from the design because of operational concerns without considering adverse effects to design and safety functions.

The availability and adequacy of design documents (1) form the basis for future plant modifications by quantifying the design margins and defining the operating envelope, (2) form the basis for Title 10 Code of Federal Regulations (10 CFR) 50.59 safety determinations, and (3) form a living record of the as-configured plant. The industry's heightened awareness of this problem prompted many licensees to review their design bases and reconstitute missing information. However, identification of design bases and reconstitution of missing or inadequate design documents can be an extremely costly process and must be balanced against the increase in plant safety. Experience has shown that the availability of design documents is an invaluable aid in making decisions that support plant operations and maintenance. These design documents also will form the baseline for future plant modifications. Until recently, however, there has been no clear consensus as to what the term "design bases" means: what comprises the minimum set of design documents necessary to support plant operation and meet the demands of the design change and configuration management process, and what priority should be placed on the regeneration of missing design documents.

1.2 Purpose and Scope of Survey

An underlying consideration in the discussion of design bases, design documents, design change control, and physical conformance of the plant to its supporting documentation is configuration management. Simply put, configuration management is the control of interfaces between various utility organizations (such as the technical disciplines in the plant design organization, licensing, operation, maintenance, design change, administration, and management) with the end result being that the as-built facility is continuously maintained and operated in accordance with its design bases. This integrated process generally has not been found at utilities until very recently. Programs to define and institute configuration management processes appear to be an industry priority. If sufficient design documentation does not exist, the success of these programs will hinge largely on the success of (1) the design-document reconstitution program to reestablish design bases and recreate, as appropriate, design documents that demonstrate the as-configured plant conforms to the design bases and (2) design-change control programs to maintain the plant configuration.

As a result of the apparent differing philosophies and approaches to programs for design-bases documentation, the NRC initiated a survey of several utilities to ascertain the availability of design documents in the nuclear industry to gain an understanding of current design-change control programs and practices and, where possible, to review and evaluate existing design-document reconstitution programs.

The survey team gathered information from a representative cross section of operating power plants, including those that have recently received operating licenses as well as older plants that have a longer operating history. On the basis of this information, the team assessed each utility's design-change control and design-document reconstitution programs.

Surveys lasting 2 to 3 days each were conducted at six utilities and at the office of one nuclear steam supply system (NSSS) vendor by a team of NRC and NRC consultant personnel. The team surveyed the mechanical/nuclear systems, mechanical components, electrical power, and instrumentation and control disciplines. Key technical personnel in each engineering discipline as well as key management and plant personnel were interviewed. Documents and drawings typical of the utility's design documents were e[illegible]mple basis. A small sample of plant modifications also wer[illegible] examine each utility's design-change control program. Utility [illegible]sentations on engineering controls, configuration management, and design-bases reconstitution programs proved helpful to the team in gaining an understanding of the overall utility design management program. The survey included design control aspects because of the close interrelationship with the design-bases activities. For example, the utility controls that have been employed in the configuration management area will have a direct bearing on the need and ability to reconstruct the plant design bases. An overall perspective of the design control environment is provided so that the design-bases reconstitution discussions can be viewed with regard to current utility practices.

Utility responses to the survey questions (see Appendix A) enabled the team to gain a detailed understanding of each utility's design-change control program. The use of discinline design-attribute matrices (see Appendix B) helped the survey team gain an understanding of the status of design documentation at each organization surveyed.

The survey had the following objectives:

- Identify the utility definition and scope of design documentation for its facility.

- Identify specific design documents that the utility uses to support plant operations and maintenance and that form a basis for future plant modifications.

- Determine the utility's control of and use of design documents, including

    - location, availability, and appropriate use of design documents by engineering, operations, and maintenance personnel

    - degree of control by engineering procedures and the scope and effectiveness of these controls

- those documents that are controlled and maintained to show the as-built plant design

- Identify the scope of the utility's program, if any, to define, reconstitute, and maintain the plant design bases and supporting design documents, including identification of

  - level of commitment and incentives for reconstituting design documents

  - scope of system-oriented and topical design-bases documents (e.g., environmental qualification of equipment, fire protection, and single failure) planned for reconstitution

  - types of documentation to be included in the utility's program and the specific design documents to be reconstituted for design attributes covered by the design-bases documents

  - priority and rationale for reconstitution of specific design documents (e.g., design input, design process, and design output documents)

On the basis of the information gathered during the survey, the team assessed the following areas:

- utility design control and configuration management programs

- the types of design documents to be controlled and maintained as-built to support plant operations

- the types of design documents to be controlled but not to be maintained as-built

- the conditions that determine which missing design documents are regenerated, the priority for regeneration of the missing documents, and the reportability requirements associated with missing design documents and with design discrepancies

- the need for additional regulatory or industry guidance regarding design document availability and control

1.3 Design Bases Versus Design-Document Reconstitution Programs

There has been much confusion regarding terminology, in particular, what is meant by design bases. The NRC inspections discussed earlier in this report and other similar inspections at different plants led to the conclusion that many plants had unretrieveable, undocumented, or incomplete design bases. This means that plants had insufficient design documentation to support the as-built facility. Since these inspections focused on systems that had been modified from the original design, the original design documents (e.g., calculations and drawings) formed the design bases or point of departure for subsequent modifications. Therefore, if engineering judgment was used as the point of departure for a modification, rather than the original design calculations because they were unavailable, the modification was said to have an undocumented design bases.

However, the definition given in 10 CFR 50.2 states that design bases are "information which identifies the specific function to be performed by a structure, system, or component of a facility, and the specific values or ranges of values chosen for controlling for parameters as reference bounds for design." This has caused some utilities to infer that in order to have an adequate design bases it is only necessary to define the functions performed by systems, structures, and components and the values or range of values for controlling parameters, without the supporting engineering or design analyses.

There are three categories of design documents. These are design inputs, design analyses, and design output documents, and all are necessary to have a fully documented and auditable design. In view of this and to avoid further confusion, the survey team has consistently referred to utility programs as "design-document reconstitution programs" throughout this report and not as "design-bases programs." However, the team has retained the term "design-bases document" (DBD) for individual system and topical DBDs because it is so widely used and understood in the industry.

1.4 Engineering Design Bases

The design bases for a structure, system, or component identifies the specific functions to be performed and the controlling design parameters and specific values or ranges of values for these parameters. From a licensing point of view, the design bases of a facility are a subset of the current licensing bases and are contained in the FSAR and other docketed information used by the staff in judging the acceptability of a facility vis-a-vis the health and safety of the public. For the purposes of this report, the team has defined a new term, "engineering design bases," to include both the design bases as defined by 10 CFR 50.2 and other design considerations implemented to optimize the system design for operational, maintenance, procurement, installation, or construction reasons. As used in this report, the term "engineering design bases" refers to the complete "engineering design bases" of the facility and includes the entire set of constraints imposed on the design (e.g., regulatory requirements, system functional requirements, conformance to accepted industry codes and standards, licensing commitments, vendor interface requirements, and other design considerations that could be classified as "generally accepted good engineering practice"). As used in this report the term "design bases" is considered to be equivalent to "design input" as defined by the American National Standards Institute in Supplement S-1 to ANSI NQA-1-1989, "Nuclear Quality Assurance Program Requirements for Nuclear Facilities," or in ANSI N45.2.11-1974, "American National Standard Quality Assurance Requirements for Nuclear Power Plants."

As stated above, engineering design bases are not limited to design features or considerations that are necessary to satisfy regulatory requirements. For example, the heat exchanger in the residual heat removal (RHR) system may be sized to cool down the reactor coolant system to the refueling temperature within a specified time (e.g., 24 hours) after system initiation. This design requirement, although not safety related, may be imposed to minimize facility outage time and may be the controlling parameter in the sizing of the RHR heat exchanger. Therefore, from the standpoint of creating a practical document that is self-contained, design-bases documents should include design considerations that are safety related as well as those that are not safety related because in some instances it is economic or operational considerations and not safety-related considerations that control the design.

1.5 Definitions

Because the definitions of certain terms vary, in this report, these terms are used with the following interpretations.

Accessible Documents: Controlled documents that are readily available to engineering and plant personnel.

As-Built/As-Configured Data: Documented information that describes the currently existing characteristics of structures, systems, and components.

Configuration Management: An integrated management process to ensure that the plant's physical and functional characteristics are maintained in conformance with the plant's design and licensing bases; that operating, training, modification, and maintainenance processes are consistent with the conditions prescribed by the design and current licensing bases; and that the plant is operated and maintained within these conditions.

Controlled: Records that are within the scope of the document control program of the utility or its contracted organization and are subject to the requirements for quality assurance records specified in ANSI N45.2.9-1974, "American National Standard Requirements for Collection, Storage, and Maintenance of Quality Assurance Records for Nuclear Power Plants."

Current Licensing Bases: The NRC requirements imposed on the plant that are currently in effect. These include the requirements at the time the initial license for the plant was granted together with requirements subsequently imposed. The licensing bases are contained in NRC regulations, plant technical specifications, orders, license conditions, exemptions, and licensee commitments contained in the final safety analysis report, and other docketed licensing correspondence including responses to bulletins and generic letters. For additional guidance in this area refer to the Statement of Considerations for the proposed Rule on Nuclear Power Plant License Renewal (10 CFR Part 54) and NUREG-1412, "Foundation for the Adequacy of the Licensing Bases," dated July 1990.

Design: Technical and management processes that commence with the identification of design input and that lead to and include the issuance of design output documents (ANSI N45.2.11-1974).

Design Authority: The organization having responsibility for maintaining the design bases and ensuring that design output documents accurately reflect the design bases.

Design Bases: Information that identifies the specific functions to be performed by a structure, system, or component of a facility and the specific values or ranges of values chosen for controlling parameters as reference bounds for design. These values may be (1) restraints derived from generally accepted state-of-the-art practices for achieving functional goals or (2) requirements derived from analysis (based on calculation and/or experiments) of the effects of a postulated accident for which a structure, system, or component must meet its functional goals (10 CFR 50.2). The design bases, as defined here, is identical to the definition 10 CFR 50.2 and includes only the design constraints that are included in current licensing bases and form the bases for the staff's safety judgments (see the definition of engineering design bases).

Design-Bases Document: The encapsulation or summary of system or topical information that relates to design bases as defined by 10 CFR 50.2 and engineering design bases. These documents serve to delineate the design intent and either directly incorporate the related design documentation or are a directory to related design documentation (e.g., calculations and analyses).

Design Change: A change to a final design document that affects a system, structure, or component.

Design Document: A document belonging to the set of documents comprised of design input documents, design studies or analyses, and design output documents that specify the design of a structure, system, or component. These are the documents to which one can refer to verify that structures, systems, and components have been designed to perform their intended function within the reference bounds of the controlling parameters and that form the point of departure for future plant modifications.

Design-Document Reconstitution Program: The overall program to (1) develop summary system or topical design-bases documents; (2) conduct verification and validation activities to ensure consistency between the design-bases documents, final design output documents, and the current plant configuration; and (3) reconstitute missing or inadequate design calculations and analyses, as appropriate.

Design Input: Those criteria, parameters, bases, or other design requirements upon which the detailed final design is based (ANSI N45.2.11-1974).

Design Margin: The difference between the value of a parameter as determined by test or analysis and the design basis specified for that parameter.

Design Output: Documents such as drawings, specifications, and other documents defining the technical requirements of structures, systems, and components (ANSI N45.2.11-1974).

Engineering Design Bases: The entire set of design constraints that are implemented, including those that are (1) part of the current licensing bases and form the bases for the staff's safety judgments and (2) those that are not included in the current licensing bases but are implemented to achieve certain economies of operation, maintenance, procurement, installation, or construction (see the definition of design bas

Essential Design Documents: Those design documents that demonstrate that structures, systems, and components addressed by technical specifications will perform their active safety function and support or demonstrate the conservatism of technical specification values. Additionally, essential design documents are those necessary both for use by engineering to support plant operations in responding to plant events and for use by the operators to quickly respond to plant events. Examples of essential design documents include, but are not limited to, electrical load lists, set point lists, valve lists, instrument lists, fuse lists, breaker lists, Q lists, diesel generator load sequencing, P&IDS, flow diagrams, electrical single-line diagrams and schematics and breaker and fuse coordination studies.

Operable: A system, subsystem, train, component, or device is considered to be operable when it is capable of performing its specified function(s) and when all necessary associated instrumentation, controls, electrical power, cooling or seal water, lubrication, or other auxiliary equipment also are capable of performing their related support function(s).

Retrievable Documents: Documents not readily accessible but that can be located in utility or contractor files or archives and that contain information that is valid for use in the design or design change process.

Validation: The process of ensuring that the physical plant, the design output documents and the design-bases documents are consistent.

Verification: The process of checking that the information contained in the design-bases documents has been correctly and consistently translated from the source documents.

2 OVERALL ASSESSMENT OF UTILITY DESIGN CONTROL

This section of the report provides the overall assessment of the design practices and techniques used at the six utilities. The survey team concentrated on the manner in which design changes are initiated, processed, and pursued to completion by the various utility organizations. Utility controls on external and internal interfaces, design documents, licensing commitments, and plant operational documents are described. Assessments of the availability and retrievability of design documents and internal guidance documents for engineering design are included. For those readers desiring only an overview, Sections 2.1 and 2.2 below are suggested.

2.1 Internal Corporate and Site Engineering Interfaces

Each of the six utilities surveyed has organized its engineering activities into traditional architect/engineer disciplines (i.e., mechanical, electrical, instrumentation and control, and civil/structural engineering) with some minor variations. All of the utilities have established both corporate office engineering groups and site engineering groups for performing and/or technically managing the engineering activities required to support design modifications. The site engineering groups are either an extension of corporate engineering or they report to the plant organization rather than to corporate engineering.

The site engineering groups of the utilities surveyed, to varying degrees, are counterpart discipline organizations to the corporate engineering staff. Generally, the larger or more significant modifications are developed by the corporate office and the smaller or replacement-in-kind type modifications are developed by the site engineering groups. Site engineering assists in implementation of the more significant design modifications developed by corporate engineering. The corporate office is typically responsible for engineering standards, calculations, analyses, design specifications, and drawings. Site engineering is typically responsible for liaison with site organizations concerning construction specifications, maintenance/test procedures, and installation details.

In some cases, the site engineering staff is not an independent engineering group but rather a part of the corporate engineering group working at the plant site. Typically, the site engineering staff has the responsibility for design and implementation of smaller scope design changes and plant modifications while the corporate staff has responsibility for more intrusive, larger scope modifications. In some utility organizations, the site engineering staff reports to the plant manager rather than to the manager of corporate engineering; in other instances, a matrix organization exists and engineers that are part of the corporate engineering staff are assigned to the plant staff reporting to the plant manager. In other utilities, the operations organization has total responsibility for design and configuration control and uses the corporate engineering staff as hired consultants for specific tasks, even to the extent that the corporate engineering staff needs to compete on a cost-basis with outside organizations to perform modifications at the plant.

While an architect/engineer organizational structure generally is used, the team identified some organizational weaknesses that are noted in Section 4 of this report.

The technical (vs. administrative) involvement in the design and the depth of personnel skills varied considerably among the utilities, as well as among the disciplines for a particular utility (discussed further in Section 2.2.3).

All of the utilities surveyed established a lead engineering discipline with an associated lead engineer for a particular modification. The involvement and support from other engineering disciplines varies depending on the scope of the modification. All the utilities surveyed have internal procedures and controls to ensure that all engineering disciplines are aware of the modifications at least at the management level. Periodic meetings (typically weekly) among the engineering disciplines are conducted to ensure coordination of design packages. One utility had a list of technical issues (such as fire protection and high- and moderate-energy line breaks) requiring coordination between discipline groups. A matrix of discipline engineers is used for large, complex projects.

At one utility the survey team found that site engineering performs nearly all of the smaller modifications in-house while corporate engineering contracts nearly all of the larger modifications. As a result, the site group appeared to perform most of the utility's modification engineering while the corporate group serves primarily in a project management role. The survey team concluded that this resulted in a shallow technical involvement by the corporate staff in the design process (for example, in-house capability for seismic calculations was sparse). If two engineering groups are performing the design changes, it becomes more difficult for a utility to control its configuration. A central design organization, which minimizes the engineering performed by separate site groups, appears to provide better assurance of configuration control.

The survey indicated that (1) utilities with plants that have recently become operational have larger design staffs with more engineering disciplines and perform more fundamental design engineering in-house, and (2) utilities with plants that became operational in the early to mid-1970's tend to have smaller staffs and rely more heavily on outside contractor organizations for the more complex and involved design activities while overseeing these activities in a project management role. The increased reliance on contracted engineering organizations will tend to increase the difficulty in performing a design-document reconstitution (DDR) program since the source documents are more widely dispersed and are more difficult to retrieve. Significantly, at the time the survey was conducted, none of the surveyed utilities had adopted the corporate systems design engineer concept, which appears beneficial in centralizing the technical ownership of the DBDs. However, many of the utilities do have system engineers that are part of the plant operations staff, although they do not perform a design function. The system engineer is responsible for the material (physical) condition of the systems assigned to him/her and usually performs systems walkdowns at periodic intervals to inspect for items such as leakage, proper lubricant levels, and loose fasteners or kinked instrument tubing. At one utility surveyed, these walkdowns were performed with the participation of a representative of the design engineering organization. Although the systems engineers have a thorough understanding of how their system operates, they may not fully understand the system design and the design decisions and tradeoffs made in arriving at the current configuration.

2.2 External Corporate Engineering Interfaces

The utility's corporate engineering organization typically interfaces with the utility's licensing organization, the nuclear steam supply system (NSSS) vendor, the architect/engineer (A/E) and engineering services contractors, equipment vendors, and the utility's plant organizations that implement and are affected by design modifications.

Interface with these groups is discussed below and significant differences between the organizations are highlighted. Further discussion of the interface with plant organizations and other groups is provided in Sections 2.3 and 2.4.

2.2.1 Licensing Interface

The utility licensing organizations are responsible for maintaining licensing commitments. The licensing organization controls the utility's final safety analysis report (FSAR), distributes NRC bulletins, generic letters, information notices, orders, inspection reports, as well as other licensing correspondence and is the point of contact with the NRC. NRC generic communications are typically screened for distribution to the proper design discipline manager for disposition. Most of the utilities assessed are using, or plan to use, a tracking system to facilitate direct access by engineers to licensing commitments. The licensing commitment tracking system and the FSAR are important source documents to support the design-bases documents.

The design engineer working on a plant modification is responsible for identifying any required update to the FSAR necessitated by the modification. In most cases, the design engineer directly marks a copy of the FSAR sections and appends those sections to the modification package. Generally, the licensing group performs an independent review of the design engineer's markup to ensure completeness of the changes to the FSAR.

While the FSAR and other licensing documentation will not be a complete source of design input information, it is an important repository of design-related information that is necessary for developing the design-bases documents.

2.2.2 NSSS Vendor Interface

The utilities typically interface with the NSSS vendor in support of NSSS analyses, design-bases reconstitution, and major modifications to the NSSS. The survey team also visited an NSSS vendor to discuss the interface process.

The utilities contract the NSSS vendors to provide the assumptions and results of the major computer codes, such as transient and accident analyses; however, the utilities do not receive the methodology or the actual code. Most utilities do not have the capability to maintain these major codes. In cases where the utility no longer uses fuel supplied by the NSSS vendor, the utility has typically contracted with the new fuel supplier for these services.

The involvement of the various NSSS vendors in support of the utilities' design-bases reconstitution efforts is described in Section 3.6.

Unless separately contracted to do so, the NSSS vendors generally do not maintain NSSS design documents as-built after commercial turnover to the utility. A few limited instances were reported where a NSSS vendor had provided this service. It was often found that the NSSS drawings and documents had not been maintained as-built by the utility, with the exception of piping and instrumentation diagrams and elementary wiring diagrams. NSSS vendors functional documentation such as system design specifications are typically not well maintained, nor are vendor manuals. Documentation of past modifications that affected the design did not always contain explicit rationale for the change.

The NSSS vendors generally have limited involvement in plant modifications, except when a utility had procured specialized equipment or services for significant NSSS modifications. Even in those cases, the NSSS equipment or services are typically handled by contract organizations, within the NSSS vendors organization, not responsible for the original NSSS design. These contract organizations may not have enough NSSS design insight to ensure that the engineering design bases have been maintained.

Extensive efforts will be required to overcome the failure of utilities to maintain the NSSS as-built design history. The reconstitution efforts in the NSSS area will involve the original NSSS vendor, alternate new fuel suppliers, and the utility or A/E that has cognizance of the NSSS modification history. Close scrutiny of NSSS design work not performed by the NSSS vendor is warranted to ensure that the engineering design bases have not been compromised.

2.2.3 Architect/Engineer and Engineering Services Interface

The utilities engineering organizations contract A/E and engineering services organizations for support in the preparation of design modifications as well as for balance-of-plant design-bases reconstitution and specialized engineering studies or services not normally found within the utility organization (for example, fracture mechanics or materials analysis).

There was a wide range among the utilities surveyed in the depth of technical capabilities, staffing levels, and the degree to which engineering work was contracted externally for the less specialized traditional engineering disciplines.

The total corporate nuclear engineering discipline staff varied from 30 to 270 between the utilities. If this is reduced to a per-unit value, the variation was from 20 to 135 employees. The percentage of work contracted externally and the supervising of contracted work also varied considerably. Generally, the proportion of modification packages performed in-house was estimated to be between 40 and 60 percent of the total, with extremes of 20 percent in one case and nearly 100 percent in another. However, when the complexity of the modification packages was considered, the proportion of those done in-house was lower. Thus, it appeared that the involvement of many utilities is more directed toward project management of contracted A/E or engineering services organizations in support of complex modifications with the bulk of utility technical effort concentrated on smaller, simpler modifications and other engineering efforts in support of plant operations. For example, the survey team found that some utilities have no capability for performing piping stress analysis in-house and rely on external design organizations to provide such analyses, using the contracted organization's procedures and design standards. Because of the wide variety of staff capabilities and engineering involvement, the survey team developed the following organizational classification scheme.

- Category 1: The utility has an extensive discipline-oriented staff in-house, and the staff has breadth and depth of engineering skills and knowledge. Mature design specifications and engineering procedures are maintained. Most engineering is performed in-house. The utility has the technical capability to develop major modifications with only specialized contracted support. The utility has high technical involvement in the work.

- Category 2: The utility has full breadth of engineering skills and knowledge in-house, but not the depth of Category 1 in all disciplines. Mature design specifications and engineering procedures are maintained. The utility has the capability to develop extensive preliminary engineering for modifications in-house, although implementation of pre-engineered packages may be contracted externally. The utility has high technical involvement in the work.

- Category 3: The utility has limited breadth and depth of engineering skills and knowledge in-house. A limited scope of design specifications and engineering procedures exists in-house. The utility serves as technical project manager with a contracted engineering service organization and has limited technical involvement. The contracted organization generally uses its own procedures manual.

The survey team concluded that it may be difficult, but not necessarily unacceptable, for a utility to operate as a Category 3 organization. However, the methods by which a Category 3 organization ensures that the engineering design bases are not abrogated during modifications and that right questions are asked during the development of modifications and that the answers are properly derived will be different than for a Category 1 or 2 organization. Conversely, operating as a Category 1 or 2 organization in itself will not guarantee successful design control unless factors such as discussed in this report are considered.

The ability of the utility to carry out a design-document reconstitution program will depend significantly on the level of in-house capabilities as defined by the three organizational categories. While the Category 1 staff should have more wherewithal and greater availability of source documentation, the Category 3 staff will possibly have the most to gain from becoming actively involved in the DDR process. The involvement of utility engineers should lead to greater understanding of their plant's design characteristics and should provide the opportunity to expand the amount of accessible design documents that will be of value for future modification design activities.

2.2.4 Equipment Vendor Interface

The utilities mainly interface with equipment vendors during the procurement process. There appeared to be little difference among the utilities surveyed, although there were some differences in the degree to which utilities maintain vendor manuals consistent with the as-built facility.

Utilities generally consult with the NSSS vendor and subvendor when modifying or replacing major equipment. However, the NSSS vendor included in the survey expressed concern that a utility might not be aware of the availability of newer and better parts for use in the NSSS vendor's equipment if the utility dealt directly with an original equipment subvendor when replacing parts.

The long period of time that has elapsed since component design and procurement may aggravate the ability to reconstitute the associated design input information.

2.2.5 Plant Interface

The corporate engineering organization interfaces with plant organizations during the design modification process. However, there was little evidence of proactive interface between the corporate and plant organizations for plant studies not directly related to a planned modification.

During the design process, most of the utilities surveyed have two formal design review meetings (all utilities surveyed have at least one) between the design organization and the site organizations to review the modification under development. These meetings occur at different stages in the design process depending on the utility, but one is usually held early in the design process (20 to 50 percent completion) to resolve issues or conflicts involving design, implementation, construction, procurement, maintainability, safety, operability, health physics, cost, scheduling, or startup, as appropriate. The second meeting may be held toward the end of the design process (90 percent completion) to ensure that no problems exist with constructability, operability, or maintainability of the modification and that new problems will not be created for plant personnel after implementation. Reviews and comments are formally documented and conflicts resolved before the modification package is approved and issued. The utilities reported that these meetings are very valuable to the design development, promoting understanding of the modification and its effect on all site organizations, and enabling resolution of most problems before implementation.

The plant interface reviews generally are conducted by the plant systems engineer. All of the plant organizations affected by the modification establish review teams. During the plant reviews, the corporate design engineering organization is essentially in a contractor role relative to the plant organization.

The level of plant experience acquired by the design engineers within the utilities' corporate engineering organizations varied among the utilities. For example, some utilities have design engineers with sufficient experience to directly mark up and prepare installation or test procedures with little further effort required by the plant organization; others do not have this level of experience and leave detailed preparation to the plant organizations.

2.3 Document Control

One element of design control and configuration management programs is a document control program that controls revisions to documents that show the as-built configuration of the plant and makes these documents available to engineering and plant personnel for use in preparing design modifications. Some utility procedures for handling controlled documents specifically address ANSI Standard N45.2.11-1974. This standard specifies methods for document control of changes and distribution. Types of typically controlled documents are listed below.

- design drawings, including those provided by contractors
- procurement specifications

- installation specifications
- system descriptions
- safety analysis reports
- environmental reports
- administrative, design, installation, and testing procedures
- design calculations and analyses
- design-bases documents
- vendor instruction manuals and drawings
- interface documents
- revisions to design documents
- field change requests
- design change requests

Most of the surveyed utilities maintain a controlled copy of plant design documents to ensure that they reflect the as-built configuration of the plant with the possible exception of piping area drawings, procurement and construction specifications, original vendor drawings, or other historical records. Many of the utilities do not update controlled calculations to incorporate minor changes or track these minor changes so that they can be assessed in aggregate to determine the total impact on system or component performance. A few utilities surveyed maintain a controlled copy of every design document affected by a design change. Those utilities surveyed that have DDR programs plan to control the topical and system DBDs, which they are currently preparing, to ensure that these documents will reflect the as-built configuration of the plant.

The utilities indicated that the types of documents listed below typically capture the design bases for the plants and serve as the basis for the design change process.

- design-bases documents
- Q-list (listing of safety-related components)
- engineering correspondence
- NSSS vendor, A/E, vendor, and utility design documents such as engineering calculations, drawings, specifications, and internal design standards and procedures
- FSAR, including outstanding updates
- operating license, including Technical Specifications
- NRC safety evaluation reports
- general design criteria (10 CFR Part 50, Appendix A) and other NRC regulations
- licensing correspondence and regulatory commitments
- environmental, State, and other regulations
- NRC Standard Review Plan

- regulatory guides
- industry standards
- analyses and test reports

Each of the utilities has several data-base management systems and other information systems that can be used to retrieve information to be used by the design engineer. These systems typically provide information on components and other plant equipment, drawings and drawing changes, calculations and analyses, design documents, a list of safety-related (Q-list) components, and plant modification status. Several utilities noted their intention to develop a configuration management information system (CMIS) that would provide an integration and control of the information contained in the other data bases and information systems.

The team reviewed one CMIS that is under development and is designed to have one primary data base keyed to the component tag number with a number of secondary data bases that can be accessed for additional component and design-bases information. The goal is to provide a system for the controlled maintenance and use of configuration data. Among the data bases planned are the Q-list components, valve list, hanger list, equipment list, instrument list, tag number versus procedure number, tag number versus drawing number, text contents of DBDs, annunciator list, and tag number versus technical manual number. The CMIS was demonstrated to be a very capable and useful tool. The configuration data in the CMIS is accessed from a carousel-type array that allows great expansion of data availability coupled with rapid retrieval of information. The utility indicated that continuous interaction of the utility personnel and the computer system designers was necessary to achieve a truly useful, user-friendly system that met their needs.

An established broad range of controlled as-built documents will aid the reconstitution of the plant design bases. The verification and validation efforts associated with design-bases documentation will be impeded if the source documentation has not been maintained in an as-built condition. The DDR program in concert with ongoing configuration management efforts can prompt the expenditure of resources to attain consistency between the design documents and the plant configuration.

2.3.1 Drawings

Plant drawings are an essential part of a document control program because they are critical to design engineers, plant operators, maintenance and technical staffs, and others in performing plant modifications and normal plant operational evolutions, in developing procedures, and in coping with off-normal operating events. These drawings provide needed design information, but become untrustworthy when they are not maintained consistent with the as-built plant design. Timeliness of updating drawings is a difficult task, but is necessary if the needs of the designer and the operator are to be met.

All of the utilities surveyed have experienced difficulty with drawing maintenance. Categories of drawings, such as logic drawings, instrument loop drawings, and piping area drawings, have not typically been maintained as-built and can only be provided through a reconstitution program. In some instances, drawing update programs in the past only caught up to a certain point and did not provide a mechanism for continued updates resulting from future plant changes. Drawing update priorities were not well defined, resulting in an overload for the drafting organization and missed update schedules. It is important that control room drawings are always updated before a modified system is returned to operation because this could result in unsafe operations and disagreements between procedures and referenced drawings.

The utilities surveyed have drawing control programs that address revisions resulting from design changes or modifications (including interim or special drawings particular to the modification or change) and revisions resulting from minor deficiencies or nomenclature errors that are not design related. The drawing control programs encompass NSSS vendor drawings, A/E drawings, plant equipment drawings from other vendors, and utility-produced drawings for the plant. One utility has identified 165,000 drawings associated with its drawing control program.

Each of the surveyed utilities has established a priority categorization for updating drawings and has identified timeframes for accomplishing the update of the drawings in each category. The number of categories vary from two to five, and the timeframes for updates vary from 5 to 14 days for the highest priority drawings (e.g., control room drawings that are required to be updated before acceptance for operability) to 180 days following a declaration of system operability or a request for updating on the lowest priority drawings. An example of a drawing prioritization method is described in Appendix C.

Although control room drawings have the highest priority for updating, only a limited number of drawing types are classified as control room drawings. Other drawings have a longer update timeframe, and the team noted instances of maintenance and operations personnel experiencing difficulties in determining the appropriate plant configuration to perform such operations as electrical system tagouts. An associated problem arising from the extended update time was the existence of some individual drawings with as many as 15 to 20 design changes outstanding against the drawing, with some implemented and some yet to be implemented. Further refinement of drawing categories in some instances may be necessary to better minimize operational, maintenance, and design control problems.

Control room drawing types considered critical to plant operations varied significantly from utility to utility. The drawing types that utilities typically update before turnover of the modified systems to plant operations as well as additional drawing types that are important to operations and located in some of the control rooms are listed below.

- piping and instrumentation diagrams (P&IDs) or equivalent
- control logic diagrams
- electrical one-line diagrams
- instrument functional loop diagrams
- control wiring diagrams, elementary wiring diagrams, or schematic connection diagrams

- electrical distribution and panel arrangement drawings
- reactor protection and safeguards drawings
- circuit breaker list or interruption diagrams
- level-setting diagrams
- three-line electrical diagrams
- ac and dc 480-volt and 125-volt feeder diagrams
- general arrangement drawings
- valve index
- instrument index
- lighting drawings
- piping schematics
- internal wiring diagrams
- instrument block diagrams

The survey team found utility programs that did not require all drawings designated as control room or operations drawings to be redrafted before modification turnover. Interim as-built temporary drawings were supplied for operations use until the drawing revision process was complete, usually within 30 to 90 days of modification turnover. Updating of critical plant drawings for operations use as a condition of modification turnover is an important function. Further refinement of drawing categorizations and better definition of priority drawings should be considered to enable timely updating of important drawings.

Some of the utilities said that they are maintaining all of the plant drawings to reflect the as-built configuration of the plant, while others said they try to maintain all but a few drawing types with the as-built configuration. The exceptions are usually historical drawings such as those contained in vendor manuals or used for a one-time or temporary application, piping area drawings, and equipment plan and general layout drawings. Key drawings are extracted from the manuals and placed in the drawing control program separately from the manuals.

Most utilities produce interim drawings in one form or another for use in modification packages, with the areas affected by the modification noted on the interim drawings. In one utility surveyed, the original drawing is marked to indicate that a modification is outstanding so other modifications can be properly coordinated. Interim drawings are issued with the modification package and as aperture cards to be included in the computerized drawing control system along with the original drawing. In other utilities, the control and status of interim and revised drawings are sometimes accomplished by means of a computerized drawing control tracking system, which would be more compatible with the integrated CMIS.

There are several unique drawing types for plant operations or modifications. Composite construction drawings that cover several modifications or field revisions are developed to show the effect of planned work on a system or area of the plant to minimize interference and modification interaction during plant outages. Composite drawings are developed for wiring and tubing modifications to provide an overview of the modification by showing interface and interconnection points of existing systems. Drawings that are composites of plant safety system P&IDs and logic diagrams are used as control room drawings critical to plant operations. Drawings that show the configuration on which the design was based are included in electrical and instrumentation and control design change packages so that the actual field condition can be verified before the modification is implemented.

While utilities have established prioritization categories to guide the drawing update process, the survey results indicated that some drawings have been inappropriately categorized and the delayed drawing updates have negatively affected the conduct of plant activities.

2.3.2 Calculations

Another class of design documents is calculations or analyses. Calculations demonstrate in an analytical fashion that the facility structures, systems, or components can meet their engineering design bases and perform their intended safety functions. Calculations and analyses are not generally considered design input documents, but often these calculations form the point of departure for plant changes and modifications.

The survey team reviewed the availability of original plant calculations and the adequacy of the original plant calculations in light of regulatory and system changes since plant licensing. They reviewed the control of changes and revisions to these calculations arising from the design change and modification process, the philosophy toward missing calculations and the priority for regenerating calculations, and the tracking of and accounting for incremental changes to system configurations that may reach a threshold necessitating a revised calculation to ensure the design bases (including the required margin of safety) are maintained.

Many of the plants have designs that pre-date the requirements of Appendix B to 10 CFR Part 50 and the specifications of ANSI Standards N45.2.9-1974 and N45.2.11-1974. As a result, availability and control of design calculations in the time preceding these regulations and standards were much less than during periods following the imposition of these requirements. Utility design-document reconstitution (DDR) programs have resulted in accessing thousands of design documents and pieces of correspondence from the NSSS vendor's files, original plant A/E's files, and utility's files. Some calculations cannot be traced to a particular system or component, or it cannot be determined if the calculation was the latest revision applicable to the system at the time of the plant operating license. Most utilities with early plants did not appreciate the need for turnover of plant design documentation from A/E and NSSS vendor files to utility files at the time of plant licensing; nor did they anticipate the need to establish and maintain configuration control of the documentation in their files following plant licensing.

However, current utility design change/modification procedures address in detail the control and revision of calculations. Some utilities revise existing calculations while some perform new calculations, leaving the existing ones in place as a historical record. When minor changes were performed on a system (e.g., replacement of a tee with an elbow in a piping run, weight change resulting from valve replacements, pipe hanger modifications, and rerouting of cable trays), evaluations and justifications for not revising calculations were usually noted in the modification package, but were not generally noted on the affected calculation to indicate that the calculation was no longer representative of the as-built system because of modifications. An instance was found, however, where procedural guidance exists for calculation addenda to summarize such minor changes so that later calculation revisions can account for these minor changes. In some cases, performing calculations to determine the effect of minor system changes may not be necessary as long as testing (such as flow testing) can adequately confirm the capability of the modified system to perform its specified function and meet the design requirements.

Some utilities do not maintain generic files of calculations, but maintain the calculations with the design modification package. In one instance, contractor organizations are relied on to prepare design modifications and to control calculations under their program, leading to potential inconsistencies in calculation control.

The survey team reviewed the identification and tracking of multiple incremental changes to calculations for which each change in and of itself might be inconsequential to the results of the calculation, but the cumulative effects might be of sufficient significance to warrant revision of the calculation to account for all changes. None of the utilities surveyed has vigorously addressed this concern.

One utility expressed concern that the existence of auditable but trivial discrepancies in the plant design documentation could require excessive and physically meaningless revisions to the documents to obtain conformity. The utility believes that as the data base of design and as-built information increases, it will find a substantial number of minor inconsistencies between documents that would be very costly and time consuming to reconcile. The utility suggested one way to address this would be to develop tolerances for minor deviations in data that are within the range of calculational or installation accuracy for design and physically measurable attributes. The Electric Power Research Institute, Nuclear Construction Issues Group suggested a similar approach for piping systems in its "Guidelines for Piping System Reconciliation" (NCIG-05). The utility also suggested that judgment should be exercised in deciding which design and construction attributes are to be a part of a configuration management program because the amount of information that is controlled or that needs to be verified can increase geometrically as the number of attributes is increased. For example, many attributes can be controlled for piping supports, including weld length and size, anchor bolt characteristics, and even paint color. Some attributes have attributes of their own. For instance, some anchor bolt attributes are embedment length, thread engagement, perpendicularity to the base plate, bolt torque, and locking device type. Therefore, if it were necessary to retrieve, control, and verify every attribute for every component one would very quickly be overwhelmed with data, much of which could be inconsequential.

2.3.3 Affected Procedures

The plant change/modification packages developed by the engineering organizations usually resulted in the development of or revision to plant procedures such as installation, acceptance test, startup test, operations, maintenance, surveillance, and chemistry procedures. These procedural changes were accompanied by changes to plant training programs. Methods for preparing these procedural changes vary from utility to utility. For some utilities, the design organization has a major role in defining procedural changes; in others the design organization provides guidelines for implementation and plant organizations define procedural changes.

One method specifies that the design engineer responsible for developing the modification design package prepare a summary functional description of how system operation will be affected by the modification. In this instance, mark-ups or draft changes to the operations, maintenance, or other plant procedures are not prepared by the design organization. The plant groups are responsible for reviewing the modification, determining which of the procedures require changes, and preparing those changes. The procedure changes are identified to the project superintendent responsible for tracking the changes and ensuring they are accomplished. However, step-by-step installation instructions are provided by the design organization, along with examination and functional testing.

Another method specifies that the design engineers provide guidance for test, installation, and plant operating procedure changes, while the site installation organizations develop detailed installation instructions and work packages using the design guidance. The plant systems engineers define the required procedural changes with the assistance of the affected plant organizations and coordinate the development and implementation of those procedural changes. The plant systems engineers also define procedural requirements for post-modification testing. Development of the majority of the procedures is typically performed on site because corporate design engineers generally have limited experience with regard to plant operating requirements.

Another utility uses a plant procedures upgrade group to develop all new procedures and procedural changes, including those arising from plant modifications. Installation process sheets and installation lists are developed by the implementing organization. Design engineering provides criteria for installation, startup, and testing and provides operation and maintenance guidelines and other necessary information for use in developing plant operating manual procedural changes.

The practice of using the design engineers to provide draft plant procedural changes with the modification packages was only found in instances in which utilities have extensive plant operating experience within their design organization staff.

Plant modifications and design changes have a similar effect on the training departments. Typically, training receives copies of modification packages for review and comment during the development stage and again at final issue of the modification. Operator training requirements relevant to the modified system are determined and the timeframe for the training (i.e., immediate, before turnover of the modification to operations, or long term) are established.

Training requirements are determined for maintenance craft, installation craft, and other non-operator training programs and lesson plans are revised or developed. Special lesson plans are prepared, if necessary, for training that is required before startup or turnover of a modification to operations. Simulator changes also are determined. Training is held during the normal operator training cycle, through special training classes or during shift briefings for the operating crews.

Procedures that are deemed critical to plant operation of the modified system (e.g., operating, abnormal operating, emergency operating, surveillance, and chemistry procedures) are required to be updated, approved, and in place in the control room before the modified system is declared operable. Other procedures that are not required for operability, such as maintenance procedures, may be updated following the determination of system operability and turnover to operations. Modification control procedures at utilities require listing all revised design and plant documents in the modification package. Most utilities use the document revision list as a checkoff or use other means of tracking procedural changes to ensure all changes are implemented before the modification package is closed.

In the past, utility design organizations had not reviewed plant procedures for conformance to design requirements. However, programs are in place, or planned, in several instances, to accomplish such reviews. The greater degree of involvement by the design organization with generating plant procedures should result in fewer concerns identified during the design-bases document verification stage.

2.3.4 Retrievability/Availability of Design Documents

Each of the utilities surveyed varied in the scope and detail of its design document types because these documents were prepared by four different NSSS vendors, four different A/Es, and four different constructors to site-specific and other plant-unique design requirements. One utility designed and constructed its own plant. The original design documents for most of the plants were prepared in the late 1960's and early 1970's, while the original design documents for one plant were prepared in the late 1970's.

Technical control over plant design modifications also varied from utility to utility. Several utilities surveyed either perform most plant design modifications in-house or perform technical reviews of the plant design modifications that are prepared by contracting organizations. These utilities have also obtained all of the original plant design documents that the plant A/Es could access. Other utilities function in a project management mode and assign the preparation of plant design modifications and the responsibility for the technical adequacy of these plant design modifications to the original plant NSSS vendor, the original plant A/E, or other contracting organizations. The plant A/Es maintain the original plant design documents for these utilities, thus the utilities must rely on these organizations for information on document availability and retrievability.

For each utility surveyed, the team obtained an overview of the availability and retrievability of the utility's design documents with regard to its unique plant licensing commitments and design requirements for the electrical, instrumentation and control, mechanical components, and mechanical/nuclear disciplines.

The attributes reviewed in each discipline are tabulated in Appendix B to this report.

The utilities surveyed have adopted ANSI N45.2.9-1974 as the standard for the preservation of lifetime quality assurance records. The plant design records for plants with more recent startup dates appeared to be adequate. The design records for earlier plants do not support all aspects of the original plant design because those plants were designed and built before the requirements of Appendix B to 10 CFR Part 50 applied. Most of the utilities intend to regenerate some missing calculations to validate system design-bases documents.

2.3.5 Availability of Corporate Design Guides, Standards, and Design Specifications

An important measure of a design engineering organization's capability is the scope, quality, and maintenance of internal design guides, standards, and design specifications. These documents typically comprise specific technical guidance that supplements the general requirements imposed by industry standards and regulatory requirements applicable to the plant design. While these internal guidance documents need not represent regulatory commitments or mandatory design practice in all cases, as a minimum, they would be evidence that the organization has considered and selected alternative design approaches, and would define at least one acceptable (but not necessarily unique) approach. Such documents promote a uniformly understood design approach to ensure that higher-tier regulatory commitments and safety requirements that are a part of the plant design bases are fulfilled.

Typically, higher-tier requirements are deliberately not prescriptive in the details of design implementation. Lower-tier documents provide working-level guidance to the designer. For example, the requirement for physical separation of redundant equipment is translated into a design approach. Such plant-specific and detailed guidance is required to control the design activities to ensure conformance with the plant design bases. The utilities addressed this need in various ways. All of the utilities surveyed had prepared or plan to prepare at least some topical DBDs that are intended to be specific enough to be used directly by a design engineer for certain areas such as electrical separation. These DBDs are particularly valuable for older plants constructed before the establishment of more recent and detailed industry standards.

Some utilities believe it is sufficient to just use industry standards and regulatory requirements to control the formal conduct of their lower-tier design activities. However, it also is necessary to control plant-specific interpretation and application of these standards and to recognize that the industry standards do not cover all of the lower-tier design decisions and analyses that must be made by the engineer.

All the utilities reported the existence of other internal guidance documents known variously as design guides, standards, specifications, design criteria memoranda, engineering instructions, quality instructions, and design (drawing) details. There was a wide variety in the scope of these documents, as well as wide variation in their structure, use, and maintenance. In some cases, the documents reflect an emphasis on procurement or installation specifications, rather than design specifications. In other cases, utilities employ older corporate standards that had been developed for fossil plants without updating or tailoring them to nuclear application. Some utilities rely extensively on the design standards and practices of the A/E performing the modification work.

A summary of the design guidance topics that the utilities reported as either available or planned is provided in Appendix D. Documents maintained by contracted organizations were not reviewed as part of the survey and are not addressed in the summary. The survey team briefly assessed the scope of the utilities' documents for comparison purposes, but did not evaluate their adequacy. The topics listed are representative, but not all-inclusive of the design attributes that might require internal guidance documents.

None of the utilities have a comprehensive collection of internal engineering design guides, standards, and specifications. Some utilities seem to have a fair number of such documents in place, some utilities have comparatively aggressive plans for developing such internal guidance, while other utilities seem to be relying on a collection of topical DBDs, existing analyses, design output documents, a sparse collection of procurement and installation related guidelines, or their A/E's standards and practices.

The degree to which design-bases information has been implemented through the application of consistent design guides will have a direct bearing on the ease and ability of the utility to verify and validate the DBDs. A sufficient spectrum of internal design guidance documents also ensures better control of the activities of contracted engineering organizations. This would provide for a consistent design approach and ensure incorporation of design-bases information into the working design.

2.4 Design Control

The design control process is applied to design activities for safety-related equipment and/or systems to ensure that applicable design requirements such as design bases, regulatory requirements, codes, and standards are correctly translated into the associated design documents, such as drawings, specifications, design analyses, calculations, installation procedures, and test procedures. The current activities at all of the utilities surveyed are stated to be in compliance with ANSI N45.2.11-1974.

Most of the utilities have taken the approach that changes to installed equipment or equipment replacements will be reviewed, evaluated, and approved or rejected on the basis of an evaluation of the changes against their current licensing bases, which for the most part are the original or equivalent codes, regulations, and quality assurance requirements employed for the unit during original design and construction. If items arise that were not considered in the original plant specifications or the FSAR, an independent determination of the applicability is made. Modifications must be consistent with or exceed design requirements for the originally installed equipment.

All of the utilities surveyed have some form of centralized design organization for control of the design and design changes. This organization is discipline oriented and located within the corporate offices. However, the responsibility and authority assumed by the design organizations differed among the utilities. Some organizations assume complete authority and either perform design changes in-house or tightly control work performed outside the organization by invoking the use of utility procedures and design standards and practices for A/Es or other contractor organizations. At the other end of the spectrum, several organizations control design changes in a project management mode. The design authority is delegated to the contracted organization performing the work and little technical design review and oversight is exercised by the utility design organization.

The objective of the centralized design organization is to focus on engineering and design issues rather than operations issues and to develop and use consistent engineering procedures and technology to solve plant problems. All of the utilities stated that they have improved their means to meet this objective over the past several years and are interested in further enhancement. Several utilities have a design feedback system whereby a comprehensive data base of experience, problems, and good practice is maintained and made accessible to the engineers developing plant modifications.

Some utility personnel characterized the modifications performed before recent program improvements as generally of good quality and involving few changes in the plant design bases. The major program improvements are in administration and control of the modification process--better configuration control and increased documentation requirements and documentation control that will ensure a tighter linkage to the plant design bases.

Utilities typically have prepared detailed procedures for the preparation and control of plant modifications. Some utilities have made minor enhancements to their procedures over the years, while others have made significant changes and improvements to their procedures as late as mid-1989. The following description of a plant modification process is representative of the process followed at the utilities surveyed and serves to highlight the detailed requirements for adequately controlling design changes to a nuclear facility. Key differences in utility methods of controlling various aspects of the design change process are addressed. Generally, current plant modification processes of the utilities surveyed are sufficiently controlled by procedure so that, if these procedures are followed, plant configuration control will be maintained. The observations noted in this section may provide a basis for further enhancements.

2.4.1 Design Change Initiation

A design change is generally initiated by the plant to request engineering assistance or a plant improvement. Often, the request is linked to an integrated schedule that provides for processing technical and engineering services while prioritizing the use of resources and providing budget accountability. Many utilities designate a modification coordinator or liaison engineer, who is either a site engineer or a plant systems engineer, to coordinate the modification as necessary throughout the development and installation of the modification. A detailed screening of the work scope is performed by the plant configuration control supervisor, or systems engineer, and the proposed work is directed to either the technical organization, the site engineering office, or an offsite source. Most significant design change requests are usually not handled by the onsite organizations. Some modifications are reviewed by an interdisciplinary management review board before being approved as a plant project.

The initial screening process appeared to be a key factor in determining which proposed modifications are selected for development and implementation. All the utilities surveyed appeared to have adequate procedural controls for the design and installation of facility modifications. Many utilities have developed procedures to screen suggested modifications to eliminate quickly those that were not necessary or were not justifiable on cost-benefit bases. It appeared that utilities are coming to the realization that the easiest way to control the plant configuration is to restrict modifications to those that are essential or at least highly desirable because they enhance operation and maintenance of systems, structures, and components.

The team found that there was a correlation between the rigor of the modification screening process and the implementation of the modification. A rigorous screening process forces the design staff to do a thorough job of assessing the impact of a proposed modification on the plant operation, the potential plant interferences that needed to be considered in the modification development, the difficulty that would be encountered in installing the modification, the anticipated radiation exposure to craft personnel installing the modification, the cost of the modification, and the effect on the outage schedule. Therefore, when the utility selectively decides to implement a plant modification that has gone through a rigorous screening process there are few, if any, surprises during implementation because walkdowns have been performed and much of the interorganizational coordination has been done in order to develop the information needed to gain approval for funding. At least one of the utilities surveyed had a two-step approval process to quickly screen out modifications that were not cost beneficial before a significant amount of engineering and developmental costs were incurred. A more rigorous screening process results in better utility control of the overall modification implementation program.

The key to configuration management is to control and minimize facility changes. Examples were cited where a weak project determination process had adverse effects on schedule management and personnel morale, while a strong project determination process that concentrated on plant needs and minimized the scheduled list of low priority modifications, resulted in a high approval rate of projects and good schedule management. At least one utility periodically reviews the list of outstanding modifications and cancels proposed discretionary modifications if they have not been installed after one or two refueling outages.

2.4.2 Design Change Development

Multiple phases are often involved in the development process for those projects that are directed to the corporate engineering organizations. For example, there are four individually approved phases (i.e., project identification, proposal, project plan, and modification package) through which a design modification normally passes as it is processed from conception to a complete modification package. In each phase, the scope of the design modification is refined, the design is developed further, and plant endorsement of that design is obtained. A brief outline of the process is provided below to show how the design change process is carried out. The survey team does not intend this to represent a recommended process; rather, it is to serve as a typical example of how design changes evolve. Some utilities use as few as two phases, but most use at least three phases. Some of the intermediate phases are optional if the cost or complexity of the modification is sufficiently small or if the project is of an emergency nature.

In the first phase, the plant and the utility's corporate engineering group perform an initial screening to determine if the proposed modification is necessary and, if necessary, whether it should be done in-house or contracted to an external organization.

The second phase consists of a walkdown of the area affected by the modification to validate existing facility drawings and to note any structural details, environmental conditions or other configuration details that may need to be considered in developing a detailed proposal package. As part of the proposal package, a project summary is developed that describes the scope of the problem, the recommended solution, and the alternative solutions considered. The project summary is generally reviewed by the utility's management and other administrative and technical groups. The summary becomes more detailed as the preparation of the design modification progresses.

The project summary that the design organization prepares explains the problem history and the effects of the problem and provides an independent root-cause analysis, an outline of the recommended solution, and a list and brief description of the major equipment added or affected by the design change. The summary also describes the philosophy and major elements in the control scheme of the design change, any direct or indirect changes to the operation of affected systems, and any changes to the unit's efficiency or reliability. It provides the outage requirements and key organizational responsibilities for the interfacing portions of the plant affected by the installation and the testing requirements for the design change. Finally, the summary describes the alternative solutions that were considered but not recommended, including initial cost, any operating costs and benefits, and any effects on occupational exposure.

The proposal package also contains preliminary assessments regarding the need for a technical specification or FSAR change or a license amendment. It includes also a consideration as to whether implementation of the proposed design modification will involve an unreviewed safety question, as well as considerations such as environmental effects or unusual design or installation challenges. The proposal development up to this point represents approximately 5 percent of the total engineering effort.

It is necessary to identify design bases and design inputs in the development of a proposal package. Many of the utilities surveyed use a comprehensive design review checklist to identify appropriate design inputs, design attributes, design criteria, and design documents. For example, the design input checklist at one utility addresses applicable codes/standards, performance requirements (including operational requirements and failure effects), compatibility, installation, maintainability, test requirements, public/personnel safety, fire protection, and security. It also addresses technical topics such as dynamic qualification, electrical separation, flooding protection, human factors engineering, welding, operating experience, and computer software changes. The detailed checklist appeared to be beneficial to the design engineer.

From these design bases and design inputs, preliminary design support documents are developed and a budget package put together that identifies time and material costs for the proposed modification.

The package is then circulated for comment by the plant's modification coordinator. The coordinator resolves these comments, as required, and prepares the proposal package with any additional information for review by the plant review group (PRG), which consists of the plant reviewers or their managers. The PRG may recommend proposal acceptance, change in scope, cancellation, or deferral to management. The design organization is consulted when comments affect the technical or safety content of the proposal.

One utility has established a formal subcommittee to the plant review committee to review all design issues of a modification package. The subcommittee is chaired by the system engineer responsible for initiating the project and includes specialists from operations, maintenance, construction, and radiation protection, as appropriate. The proposal package is typically reviewed for correctness of the problem statement; adequacy of the 10 CFR 50.59 safety evaluation, equipment selection, and recommended design change; effect on plant systems during installation; requirements for system tag out during the outage; and accuracy of plant-provided design input and post-modification testing.

Some utilities have performed 10 to 30 percent of the design effort by this point in the design development process, depending on the scope of the project and the utility organization.

The project plan is the third phase of the example modification development process and forms the basis for the decision to consider funding the modification. Its primary purpose is to clearly define the recommended minimum design changes that will meet the intent of the project. The project plan also provides estimated labor and procurement schedules and cash flow requirements. It is comprised of the engineering plan, produced by the design organization, and complementary plans produced by the site and other organizations. The amount of design work completed at this stage of the modification package usually consists of adequately defining the modification and reaching agreement with the plant on the basic design. About 50 percent or more of the project's engineering and design work may be required at this time to reach the desired level of design definition. In this phase, extensive coordination between the various engineering discipline is required for complex modification.

The engineering portion of the project plan is intended to resolve design issues so that the final design, the procurement, and the modification package can be completed. Design uncertainties in the engineering plan are listed on affected drawings and documents to facilitate site consideration. These issues will either require resolution before project plan approval or later during the development of the modification. When the design organization releases the modification package to the site after an independent design review of calculations has been performed, there are usually no outstanding issues that require resolution before site approval and issuance for implementation.

The engineering portion of the modification package includes the traveler (the cover sheet for the modification package), the project summary, the design support documents, and design drawings, and the budget package. Design support documents include a preliminary safety evaluation; a design-bases document; lists of valves, motors, instruments, lines, and other significant equipment; a cable list; a bill of materials; a list of spare parts, and plans for installation and testing.

The design-bases document incorporated in the modification package is prepared for those projects involving design changes or installation methods that are anticipated to affect safety-related structures, systems, and components (SSC). The document contains applicable design inputs such as design bases, regulatory requirements, safety analysis report, and technical specification requirements, as well as codes and standards for those SSC to be modified or added. If an applicable design-bases document already exists either through a DDR program or through development for a previous modification package, reference and revision may be made to the existing document instead of creating a new document.

Using the engineering plan, the plant and support organizations develop complementary plans for fabrication, installation, training, simulator modification, testing, and closeout. The design organization integrates the complementary plans into the complete project plan.

The integrated project plan is then submitted to the PRG for review and approval. Unresolved issues that will require site concurrence for resolution, are listed with the party responsible for resolution, the party from whom concurrence is required, and the forecast schedule for resolution.

Once the project plan is approved, the design organization must produce final design documents and drawings consistent with the plan and the site is required to commit to the design plan so that additional requirements will not be imposed during or after design completion. This approach reflects the concept of the plant as a customer and the engineering organization as a supplier of materials and services.

The fourth phase is the modification package phase and represents the culmination of the design change process. The package contains the traveler, project summary, design-support documents, design drawings, installation instructions, testing requirements, documentation revisions, and review/comment sheets.

The traveler is the cover sheet for the modification package documenting the completion of design, reviews, and approval. The project summary specifically describes the scope of the modification. The design-support documents that accompany the modification package include design-basis documents, plant drawings, and equipment lists; nuclear safety evaluations; major radioactive evaluations according to an approved procedure; certification of seismic design adequacy; an environmental qualification impact evaluation, Q-list or marked up drawings showing safety-related (Q-list) components or boundaries; and other engineering impact evaluations required by other procedures.

Several utilities hold periodic meetings to coordinate the implementation of a modification. These meetings were usually held on site before implementation of a modification and at various stages during implementation and typically include (depending on the scope and complexity of the modification) representatives from groups such as operations, modifications, instrumentation, engineering (site and corporate), health physics, training, and construction.

Most utilities perform field walkdowns associated with the design phase of the modification. These walkdowns are performed to identify potential interferences or requirements that may have been missed by review of the design documents, identify errors or inconsistencies between plant configuration and design documents, confirm testability of equipment, and identify possible security or fire barrier effects. A formal set of walkdown questions for each of the two walkdowns may be used, with observations recorded and resolved by the design engineer.

In some cases, the walkdowns are mandatory unless waived by approval of utility management, and typically involve design engineering, operations, maintenance, construction, system engineering, and other organizational representatives as necessary. In some cases, when the decision is left to the individual design engineer such walkdowns may not be performed, resulting in a less effective modification implementation process and possible field changes required to resolve interferences that should have been identified in the walkdown.

2.4.3 Modification Implementation

The installation instructions for the modifications are developed by the design engineer and incorporated in the modification package when it is issued to the plant. The installation instructions specify any special inspections, processes, and testing requirements, including acceptance or rejection criteria not normally specified by existing programs or applicable drawings and specifications. These instructions also reference the installation-related codes, standards, specifications, and regulatory requirements that are specified or assumed as part of the design bases but are not indicated or included on drawings, reference specifications, or approved procedures.

The procedural steps provide a sequence of events and sufficient direction to perform the work. The detail of control and guidance needed is dependent on the complexity of the work, the possible effect on plant operation and operability of equipment, the documentation required, and the existence of applicable procedures. The drawings, instructions, and necessary procedures are designed to be sufficiently detailed to ensure the work is performed correctly.

At some utilities, design engineers only provide draft instructions or general guidance on the effect of the modification on work activities; specific installation instructions and work control documents are prepared by the implementing organization. The maintenance organization prepares the specific installation requirements for simpler changes or the site construction organization for changes involving major work efforts and staffing requirements.

Acceptance tests are included or identified in the modification package by the design engineer. These tests are to demonstrate that the changes made by the modification were satisfactorily implemented and to verify compliance with the required surveillances. As a minimum the tests

(1) verify that the new or modified components function satisfactorily and are adjusted properly

(2) test logic under all credible configurations within the limitations of plant design and conditions

(3) verify the performance requirements to the extent necessary to determine operability

(4) include post-maintenance tests required because of maintenance and modification-related activities performed as part of the modification work

(5) include new technical specification surveillance test requirements that result from the modification and are necessary to demonstrate operability

(6) include existing technical specification and American Society of Mechanical Engineers (ASME), Boiler and Pressure Vessel Code, Section XI, surveillance test requirements on new equipment or components as required to demonstrate operability

(7) include tests required by the codes and standards (ANSI Standard B31.1 or ASME Section III)

(8) include hold points for other prerequisites for operability not otherwise provided

(9) verify that temporary connections or temporarily installed equipment for testing has been removed

Acceptance tests include details on how the test is to be run and what constitutes acceptance. Existing or proposed surveillance tests may be used for acceptance tests. Those portions of acceptance tests that cannot be performed until after the unit or affected system is returned to service are typically identified as startup tests. Startup tests may include inservice leak tests, surveillance tests, and other tests that can only be done after the modified system has been released to operations. These tests are identified as exceptions. Some utility design packages contain only general information on testing, leaving the detailed development of the tests to the site organizations after issuance of the final engineering package.

All utilities surveyed require that modification packages contain a design document revision sheet that lists the design and plant documents known to need revision. The design engineer may provide draft changes to plant documents or the responsible plant group may prepare document changes directly on the basis of the information contained in the modification package. If the safety analysis determines that a change to a description contained in the technical specifications or FSAR is required, marked up copies of the affected pages are included in the package. The lead engineer is responsible for obtaining vendor documentation, drawings, and technical manuals for engineering-procured equipment installed for the modification.

The design organization and the plant both review the modification package for approval. The design organization performs, as a minimum, a design verification/technical review and the nuclear safety review, as well as other reviews that are addressed on the traveler. The design verification review is in accordance with Section 6 of ANSI N45.2.11-1974. This would be an independent verification performed by competent individuals or groups other than those who performed the original design. Acceptable design verification methods include design reviews and alternative calculations or qualification testing. If the design review method is chosen, it would include such things as verification of design inputs back to their source documents, review of the design methodology and the reasonableness of design assumptions and the reasonableness of design outputs relative to design inputs. The designated plant reviewers review the modification in accordance with the list of attributes specified in the modification procedure. Modifications that are determined to constitute either an unreviewed safety question or a change to the technical specifications are typically approved by the plant nuclear safety committee before final approval. The modification is then approved by plant management and distributed in accordance with plant procedures.

Modification packages are usually released to the sites 3 to 6 months before the required implementation date. Most major modifications are implemented during plant outages because systems or portion of systems are required to be taken out of service or to minimize the potential for interaction with safety system functions during operation. Most of the utilities indicated that the release of modification packages by the design organization is generally timely to accommodate plant review cycles, preparation of implementation paperwork, and procurement of equipment.

Any changes to an approved modification package are performed by field revisions. Field revisions are typically limited to changes that are within the scope of the modification package and do not conflict with any requirement or conclusion of the safety evaluation. Field changes predominantly occur during installation because of interferences or other complications that were not considered in the initial instructions. Incorporating a large number of field changes into the modification package makes it difficult for the implementing organization to confidently accomplish the work tasks. One utility surveyed requires that the modification package be revised if the total number of field changes accumulating against the package has the potential to confuse or mislead the constructor or plant personnel.

The site implementation phase of modifications normally involves work authorization, installation and inspection, acceptance testing, walkdown, installation documentation review, and declaration of operability.

The modification coordinator is responsible for coordination of work activities between the utility organizations and/or contractors involved in the modification installation. The testing coordinator is responsible for maintaining control of the system during acceptance testing to prevent misoperation.

The modification coordinator also schedules a walkdown inspection near completion of the installation. The additional participants in the walkdown are usually the systems engineer, the installing organization, quality assurance (QA) and quality control (QC), the design organization, operations, and maintenance. A detailed set of guidelines for the walkdown is provided. The walkdown consists of a field verification of the modified equipment to generally verify the complete and proper installation of the modifications. All outstanding or inadequate work items are listed on the exceptions list, and those impacting operability are resolved before declaration of operability. The modification coordinator maintains the exceptions list. Most of the utilities regard a post-modification walkdown as optional at the discretion of the modification coordinator, and when a walkdown is determined to be necessary, it may not include operations, maintenance, or design organization representatives.

The performance of the post-modification walkdown presents a unique opportunity to have a multidiscipline group review the finished product for acceptability. The involvement of operations and maintenance can augment the normal QC inspection perspective and identify operability concerns that would otherwise remain undetected

2.4.4 Modification Closeout

Several prerequisites have to be satisfied at most utilities before a completed modification can be declared operational and turnover of the modified system to operations can be completed. These include such things as completion and sign-off on all work packages, revision of operating procedures, update of control room drawings, and training of operators. The updating of control room drawings before acceptance of the system by operations ranged from red-lined drawings to totally redrafted drawings. Some utilities append drawing change notices to the control room drawings until redrafted versions are available.

Most of the utilities surveyed have a detailed process specified for closeout of modifications. One utility's process for modification closeout involves preparation of a modification completion report, QC review of the construction work procedures, verification that construction drawings are as-built, update of operating manual procedures, updates of vendor manuals, preparation of a recommended spare parts list, and completion of any additional operations and maintenance training. Review and acceptance of the completed modification is performed by a plant management committee. Design documentation is updated, generally within 3 but not more than 6 months following acceptance of the modification.

Once the implementation of a modification is completed, all installation and testing documentation is reviewed for correctness and completeness. When the review has been completed and comments resolved, the modification coordinator forwards the installation documentation package to document control.

A modification cannot be declared operable until installation, acceptance testing, documentation package transmittal, and formal declaration of operability have been completed. The scope of operability may be final operability (total scope or last in a series of partial operabilities), partial operability (less than total scope, with boundaries defined by field revision), or exception (resolution of an exception which affected equipment or system operability).

The declaration of operability by the operations organization certifies that installation activities (except for those declared as post-operability exceptions) have been satisfactorily completed; acceptance testing is satisfactorily completed (except startup tests); installation documentation packages are complete; plant documents and drawings required for operation are updated; responsibilities such as training and incorporation of the modification into plant programs have been completed; technical specification changes, if applicable, have been resolved; pre-operability exceptions are closed; and startup tests are completed.

2.4.5 Modification Interactions

Each utility surveyed has provided mechanisms to minimize the likelihood of conflicts or adverse consequences arising from conflicts between modifications that are planned or in process that may affect other planned or in-process modifications. Many utilities have systems engineers either in the site engineering organization or in the plant operations organization. As employed by most utilities, the systems engineer is an engineer generally reporting to a site organization under the plant manager. The systems engineer has the responsibility to be knowledgeable on all modifications that are being proposed or implemented on his/her assigned systems. The systems engineer usually acts as the modification coordinator interfacing between the site organizations involved in the installation of the modification and the engineering organization, either site or corporate, that is sponsoring the plant modification. In this role he/she typically assures that the work packages have been properly prepared and the work has been completed as specified by the crafts involved, that the necessary drawings, plant operating or maintenance procedures, and other plant documents have been updated as required, and that the modified system has been turned over to operations in accordance with plant procedures. The systems engineers assist in determining the impact of multiple modifications on their assigned systems.

One utility stated that its technical staff maintains awareness of potential modification interactions through project management mechanisms administered by engineering and plant staff. These include 5-year business plans; progress reports; design-control computer data bases; scheduling techniques; internal planning, budgeting, and scheduling programs; and contact with the plant systems engineers. Meetings are held between unit managers within engineering and between engineering and the site organizations to discuss planned and in-process modifications.

One utility minimizes modification interactions by using a special set of composite drawings to reflect all modifications issued against that drawing and to indicate the status of the modifications before and during the outages. This utility said this effort helped to resolve the many and complicated interfaces between extensive plant modifications.

At this utility, monthly coordination meetings are held between the general office and the site engineering organizations to cover the scope of work in which each group is actively involved. Specifically, engineers are instructed to review the interim drawing reports to ensure that any modification packages already issued would not adversely affect work in progress in the same area. Design engineers are required to reserve items such as terminal blocks, penetration points, tag numbers, and breakers and to provide modification indicators on controlled file copies of the affected drawings.

Another utility uses special designators for drawings, calculations, specifications, and other affected file documents for changes that are in process. This alerts a designer to possible changes that might affect his design when he accesses the documents. Also, if construction of a modification has not been completed within 6 months of approval for implementation, the construction drawings are reviewed to verify that no other design changes have been installed that would adversely affect the installation or testing of the modification. All affected approved design output documents are required to clearly state restrictions associated with the sequence for implementation of the modifications.

The utilities surveyed appeared to have developed mechanisms to administratively control the potential for adverse modification interaction.

2.4.6 Selection of Modifications for Implementation

The utilities all have some form of multiple-year (usually 5-year) integrated schedules for utility projects to which their proposed nuclear plant modification projects of any substantial magnitude must conform. Proposed projects are screened not only technically but also by considering the cost, priority, and importance of the project to overall plant safety and operational efficiency. Management budget committees conduct continuing reviews of each modification during its early stages to ensure costs are adequately estimated. Such a review may cause a proposed project to be deferred or cancelled. Conditions also may arise requiring completed modification packages awaiting implementation to be deferred or cancelled because of a higher priority modification.

As stated in Section 2.4.1, the initial screening process for plant modifications is a key factor in determining which of the proposed modifications are selected for development and implementation. A good screening process results in better utility control of the overall modification implementation program. One utility process for preparing a request for engineering assistance details cost and personnel resource requirements and rates the benefit of the requested work in 12 categories. These categories include nuclear accident prevention and mitigation, plant availability, avoidance of personnel error, plant reliability, and community or industrial obligations. This detailed screening enables the utility to more accurately judge the priority of the modification with regard to its value to the overall safety and efficiency of the plant.

2.4.7 Design Margins

Nuclear power plant designs of structures, systems, and components inherently contain design margins with respect to limits in industry codes and standards and NRC regulations and regulatory guides. During the plant licensing process, certain design margins may be established by the NRC either implicitly or explicitly to ensure additional plant safety or to compensate for uncertainties in the analyses introduced by simplifying assumptions.

These margins may be defined in the utility's FSAR or technical specifications, the NRC's safety evaluation reports, or other licensing correspondence. Reduction of these margins by plant licensees requires review and approval by the NRC pursuant to 10 CFR 50.59.

However, additional licensee-established design or operating margins that exist over and above those specified in licensing documents may be revised at the utility's discretion during the design-change process without the involvement of NRC regulatory review and approval. An example of this type of margin might be the installation of a new system pump that has less developed head than the previously installed equipment, but it is still capable of meeting head and flow requirements specified in the licensing documents.

2.4.8 Minor and Temporary Modifications

(1) Minor Modifications

The utilities surveyed handle minor modifications in a variety of ways. Several categorize minor modifications as those that lie outside the vital plant areas and have no effect on safety-related aspects of the plant. Others apply a 10 CFR 50.59 safety determination to determine if a safety evaluation is required. One utility instituted a procedure for minor modifications that incorporates a screening process consistent with the Electrical Power Research Institute, Nuclear Safety Analysis Center document NSAC-125, and in essence declares that the modification shall not be one that adversely affects a structure, system, or component described in the FSAR or technical specifications. If these conditions are not met, the change is processed as a modification package, even if the expenditure for the change is minor. In many instances, however, utilities do not distinguish minor and major modifications in terms of how they are handled.

Most utility design organizations prepare equivalency evaluations for replacement parts or components used in maintenance and repair activities at the plant. If like-for-like replacement parts or components cannot be obtained, then it may be necessary to use a substitute replacement item. The plant system or component design bases are considered not to have been altered if equivalency of the form, fit, function, and interchangeability (including equipment qualification requirements) of an item has been established; that is, no modification has occurred. The equivalency evaluations include comparison of the original and replacement item characteristics, determination of critical design characteristics, and consideration of failure modes, replacement parts evaluation, seismic qualification, and environmental qualification. If, however, the new item is not equivalent, a modification must be processed in the normal manner.

One utility has extended the minor modification process to address other plant changes that do not involve complex changes and do not alter existing design bases and criteria. Examples of these are material substitution, hanging and mounting of miscellaneous items, instruments and pipe/conduit supports, and administrative changes to drawings, vendor manuals, or other plant design documents.

If properly implemented, the utility controls surveyed appeared capable of controlling the degree to which the plant design is changed by a minor modification.

(2) Temporary Modifications

Most of the utilities surveyed have methods of controlling the duration of temporary modification installations.

Temporary modifications are controlled in a manner that ensures operator awareness, conformance with design intent and operability requirements, preservation of plant and personnel safety, and plant configuration control. It is intended that temporary modifications be minor in scope, of short duration, and few in number, thus minimizing excessive temporary changes of drawings and other documents. A temporary modification is defined as temporary electrical jumpers, line, or hose that is used to alter a system's configuration or that removes components within a system thus altering the system's configuration.

A temporary modification log is usually maintained by operating personnel in the control room. A cognizant engineer performs a technical evaluation; completes a 10 CFR 50.59 evaluation; develops procedural changes, if required; prepares drawing markups, if required for operations concurrence; and obtains approval by the plant nuclear safety committee before installation of the temporary modification.

Installation and removal of temporary modifications are normally performed by maintenance personnel. Verification of the installation and removal or a functional check is performed to ensure correct operation of the modified or restored system.

At one utility, temporary modifications are resubmitted to the plant safety committee for authorization to remain installed after a duration of 6 months.

A cognizant engineer is required to make a physical check of each accessible installed temporary modification to ensure proper installation, presence of tags, and satisfactory condition of the modification device. In another instance, the plant is required to submit a design change request to initiate a possible design change for any jumpers or lifted leads that are intended to be installed for more than 30 days.

The utilities surveyed considered strengthening the control procedures for temporary modifications as a factor in reducing the number of outstanding temporary modifications. Control of temporary modifications, historically, has been a weak area for the industry in general and is an area that needs continued attention to maintain control of plant configuration.

2.5 Control of Licensing Commitments

Most of the utilities surveyed have some form of commitment tracking system to log, track, and ensure closure of corporate and regulatory commitments. The survey team reviewed some of these systems with regard to how they related to the design control and configuration management aspects of the plants.

Technically based licensing commitments resulting from NRC bulletins and notices, licensee event reports, or corporate correspondence (such as commitments to alter the plant, its current licensing bases, or its procedures) are sometimes not entered into a data base tracking system. This made it difficult for design engineers to search for, retrieve, and review these commitments when preparing design modifications. In some instances, the licensing commitment tracking system is used to track administrative details such as the specific licensee correspondence that responded to NRC bulletins, generic communications, and inspection reports.

One utility maintained two data bases, one for historical licensing commitments and another for licensing commitments currently applicable to the plant. These data bases are accessible and are used by design engineers when preparing design modifications. In addition, topical and system design criteria documents under preparation for the plant detailed the relevant licensing commitments. Another utility tracks licensing programmatic and administrative commitments in its system but does not specifically track design commitments. However, design commitments can be determined through knowledgeable individuals searching other available data bases.

Utility modification procedures generally require preparation of a safety evaluation and research of the FSAR, technical specifications (TS), and other licensing commitments as part of the design process. These documents are updated as necessary and the updates are included as part of the modification package. Current requirements for FSAR updating assist the design engineers in assuring that the FSAR is consistent with the current licensing bases; however, it should be recognized that the information in the FSAR can be as much as 18 months out of date. Therefore, it is important for a designer to look at the FSAR in conjunction with any licensee-approved changes that have not yet been incorporated. Likewise, it should be recognized that the FSAR alone does not form the entire current licensing bases for the plant. The current licensing bases are contained in docketed documents such as the FSAR; TS; safety evaluation reports; and correspondence between the licensee and NRC.

3 EVALUATION OF DESIGN-DOCUMENT RECONSTITUTION PROGRAMS

This portion of the report provides an assessment of the design-document reconstitution (DDR) programs for the six utilities surveyed and how these programs are integrated into the overall design control and configuration management process. The team reviewed the philosophy and approach of utilities to the reconstitution of engineering design bases, the level of effort expended, the output documents resulting from the programs, the schedules for completion, the involvement of original plant A/Es and NSSS vendors, and the degree of validation of the program outputs. The survey team assessed the utilities' definition and concept of design-bases documents (DBDs), their incentives for initiating design-bases documentation programs, their intended uses of engineering design-bases documentation, their reconstitution process for these documents, and the nature and depth of detail provided in the documents.

3.1 Overview of Design-Document Reconstitution Programs

The utilities surveyed are using a variety of approaches and philosophies in their design-document reconstitution programs. This is primarily because each utility has different methods for controlling the plant design and configuration, different levels of design documentation that are available and retrievable, and different goals and objectives they want to achieve through completion of their design-document reconstitution program. Because utilities have different needs and objectives, it is beneficial for them to retain the flexibility to choose the scope of their program, the program goals and objectives, and the format of the DBDs that best suits their individual needs.

3.1.1 Design-Bases Document Concept

The most common approach to DBDs in the utilities surveyed is that they are controlled documents that are produced by collecting verifiable upper-level design information into integrated documents that address either plant systems or plant generic topics (such as seismic design or electrical separation). Most utilities consider DBDs to be system or topical summaries of the engineering design bases of the plant and directories to design analyses and design output documents that demonstrate the implementation of the engineering design bases. They believe the DBDs integrate information that already exists but that is not readily retrievable or accessible to the designer. Where the engineering design bases or other design documents do not exist or cannot be found, it may be separately reconstituted and referenced in the DBD (e.g., an essential calculation might be regenerated).

Generally, the utilities use ANSI N45.2.11-1974 to categorize design documents. The three categories of design documents are design input documents, design analyses, and design output documents. Design bases are usually considered to be equivalent to the ANSI N45.2.11 definition of design inputs. The difference in DBDs produced by the various utilities was a matter of document structure, varied emphasis on engineering design bases versus configuration, depth of detail, depth of cross-referencing to other design documents, and degree of verification or validation. The general intent of the utilities in developing their DBDs is to provide fundamental design inputs (such as codes, standards, regulatory requirements, and analytical assumptions) and a varying degree of cross-referencing to design analyses (e.g., calculations, trade-off analyses, evaluations) and design output documents (e.g., facility drawings and procurement documents). Unless otherwise indicated, this interpretation of DBDs is used in this report.

Although the utilities used various names for their DBDs, including "design criteria memoranda," "enhanced DBD," and "analytical DBD" and the emphasis on the DBD content regarding the inclusion of different types of information also varied among the utilities, most of the DBDs reviewed contained the following information:

- system-specific regulatory requirements and exceptions
- system-specific licensing commitments and exceptions
- supporting documents containing design information (e.g., drawings, calculations, procurement documents, and correspondence)
- system functional description and engineering design bases
- component descriptions
- system and component testing requirements
- functional requirements for support systems
- system instrumentation and control requirements

Some DBDs contained the following additional information:

- description of system and component design limitations and operational considerations and restrictions
- historical summary of system modifications and why they were made
- description of how regulatory design bases were met
- list of open items to be resolved as part of the DDR process
- description of system and component design parameters and why they were selected
- system-based success trees that define the sequence of functions that need to be completed for successful operation of the system
- system-based logic trees for each system operating mode to define
    - design bases and regulatory requirements
    - system safety function
    - system parameters
    - component parameters

- design bases for safety-related structures

- design bases and assumptions used in the FSAR Chapter 15 analyses

- operational conditions matrices to define

  - component operation during different plant operating and accident conditions
  - system operating conditions during plant operating and accident conditions

- system responses to plant transients and accidents

- specification of design margins

- system-specific responses to postulated failures during different plant operating modes

- reasons for set points and alarms

- system-specific calculation summaries including significant assumptions and conclusions

The utilities expressed different viewpoints with regard to what constitutes design inputs, particularly as related to information contained in the FSAR. The general consensus among utilities is that some information contained in the FSAR is provided to assist the NRC staff in understanding the design or function of a structure, system, or component. However, in the opinion of many licensees, such information provided for descriptive purposes does not form a part of the current licensing bases and should not be identified in a DBD. Although certain information may have been included in the FSAR as descriptive information, it is extremely difficult to partition the information in the FSAR into that which represents regulatory commitments and that which represents descriptive information. As presently defined, all the information presented in the FSAR as well as other docketed information is part of the current licensing bases. In addition, to limit the information contained in the DBDs to only that information that supports the current licensing bases would limit the usefulness of the DBDs since some design criteria or engineering design bases were imposed for economic reasons or to achieve perhaps greater operational flexibility. It is important that the DBDs contain all the rationale used in arriving at the final design, not just those dictated by regulations or regulatory guidelines. In some cases, it was the engineering design bases that were the design limiting considerations; inadvertently abrogating these assumptions could affect the ability of the system to function when challenged.

One fact that became clear as the survey progressed was that each utility had different needs with regard to design-document reconstitution depending on the utility's organizational structure, the age of the facility, the design documentation that was originally purchased from the A/E or the NSSS vendor, the amount of engineering that was done in-house, and the degree to which design documentation was maintained current and the ease with which it was retrievable. In addition, to the obvious purpose of compiling engineering design-bases information and recreating certain design documents, utilities had other objectives that they wished to accomplish by their DDR program, such as the support of anticipated plant life extension activities or to provide engineering design-bases information to their operating and maintenance personnel. Therefore, although all DDR programs may contain many of the same elements, each utility needs to develop a program that fulfills its unique needs. For this reason the DDR program for each facility will be somewhat different as will the format and content of their DBD documents. Several examples below demonstrate different approaches and conclusions reached by utilities on DDR programs.

On the basis of the results of a prototype DBD program, one utility believes that it has sufficiently comprehensive, controlled, retrievable, and accessible design documents. Therefore, the utility has determined that the investment necessary to produce system DBDs is not justified. This utility claims that its existing design documentation, internal procedures, configuration management, and document retrieval/access system is sufficient for maintaining the engineering design bases. The prototype DBDs, developed by a contractor, appeared to the utility to be embellished system descriptions with little perceived value. Consequently, this utility does not plan to develop any system DBDs but is developing a limited number of topical DBDs (addressing, for example, electrical separation and issues related to Appendix R to 10 CFR Part 50).

Another utility that believes it has a complete set of design documents and an adequate system for keeping design documents current has a DBD program that is directed at increasing the awareness of plant organizations to design considerations in order that operations personnel can better understand the types of changes, for example, to maintenance or operating procedures, that constitute design changes and require engineering review and approval. This utility considers the DBD to be primarily a training tool to promote an awareness of the plant engineering design bases within the plant operations and maintenance organizations. In contrast, other utilities cited engineering as at least one of the primary users of the DBD, particularly for the preparation of design modifications.

The fundamental engineering design bases for important aspects of recent designs were often established in earlier NSSS vendor and A/E design evolutions when documentation requirements were much less rigorous. Also, utility organizations tend to evolve from a design orientation to an operations orientation over the operating life of the plant, which makes the definition and maintenance of the plant engineering design bases important. In addition, utility staff turnover as a result of retirement or other reasons makes the preservation of design information in a retrievable, user-friendly format a necessity. Utility programs conducted to date in conjunction with industry configuration management programs and the continued findings of NRC inspections indicate the value of adequate definition and maintenance of plant engineering design bases both from the benefits to plant safety and the efficiencies achieved in designing and reviewing proposed plant modifications and performing licensing reviews. Continued decline of the corporate memory of the NSSS vendor, the original plant A/E, and the utility through personnel attrition will make the DBD development process more difficult the longer it is delayed.

3.1.2 Incentives for Initiating Design-Document Reconstitution Programs

The driving force behind the development of many of the DDR programs has been NRC inspections that found licensee deficiencies and weaknesses in adherence to, or knowledge of, the engineering design bases. The DDR programs have often been coupled with other utility programs to improve configuration management of the plant. With one exception, the plant DDR programs started with a pilot phase that addressed two or three systems and then progressed to a more intense effort once the pilot phase had been completed. The utility fully defined the objectives of the program and the lessons learned during the pilot program were incorporated into the final DDR program. A well-managed DDR program is expected to take 3 to 4 years to complete, including verification of the DBDs and validation to ensure that the facility agrees with the engineering design bases and other design documents. The DDR program will provide a documented reference for engineering personnel to use that will facilitate and support many operational and licensing actions, such as the development of plant modifications, the conduct of 10 CFR 50.59 safety evaluations, operability determinations, the development of justification for continued operation to support waivers of compliance from plant technical specifications and to support licensing document updates and changes to technical specifications.

In addition to pragmatic reasons for initiating a DDR program, the prime reason is the increase in plant safety gained by having a complete knowledge of the facility's engineering design bases. Although the increase in safety is an intangible benefit because it may be difficult to measure in the short term, in the longer term the increase in safety should become apparent from a review of operational data.

3.1.3 Intended Use of Design-Bases Documentation

Of the six utilities surveyed, all have some level of a DDR program in place. One utility reported that the plant organizations are intended as the primary user because the engineering organization uses other documentation and the DBDs do not provide any additional information or insights for that organization. Of the five remaining utilities, most intend the engineering organization to be the primary user and the remainder assign roughly equal importance to engineering and plant organizations as users of the DBDs. Plant systems engineers, for example, may use the DBDs as the basis for validation of system performance. One utility specifically defines the user to be a graduate engineer having 2 to 3 years experience who is knowledgeable in theory but not necessarily knowledgeable in the engineering practices employed at the time the plant was designed. Again, because of the unique needs of each utility, it is important for each utility to target the end users of the DBD during the pilot phase of the DDR program to identify the specific objectives to be achieved. Training and involvement of engineering and plant personnel in the use and development of DBDs will be required before DBDs become significant enhancements to design control.

3.1.4 Design-Bases Document Development and Design-Document Reconstitution

The utilities surveyed have different approaches toward developing DBDs. One good approach toward engineering design-bases reconstitution is a template approach. The utility begins with a specific list of design attributes, specific values or ranges of values for controlling design parameters, analyses, calculations, and documents that it believes to comprise or support a complete engineering design bases. One utility surveyed used the template approach to identify the values or ranges of process parameters that should occur at the design conditions and the system actions that need to be completed for the system to perfom its intended safety function. These were developed in the format of success trees and design-bases functional diagrams. An example of these is provided in Appendix E. From these success trees and design-bases functional diagrams, the important system parameters and operations can be determined and the necessary supporting documentation can be identified and/or parameters can be identified for field validation.

As the utility searches, retrieves, classifies, and assesses its documentation, shortfalls relative to the template may be identified. The acceptability of the values of the design parameters documented and supported by these missing design documents are then evaluated and the need to regenerate the missing supporting design documentation is assessed. The utilities with plants that have operated for more than 10 years seem to be more aggressive in identifying missing supporting documentation. If regeneration of these documents is deemed necessary, regeneration can be prioritized on a time scale commensurate with its perceived safety significance. At least one utility uses probabilistic risk assessment to determined the safety significance of missing supporting design information and prioritizes the regeneration of missing design documentation on the basis of change in probability of core melt.

While utility DDR programs all seem to be identifying missing design documents, they are not all assessing the need for regeneration or prioritizing the regeneration. This tendency was most noticeable for important supporting calculations. For example, one utility has a completed DBD for the electrical distribution system, but complete short-circuit calculations supporting the engineering design bases of the emergency power system were not available.

An analysis-based approach is useful for developing a template of engineering design bases and design parameters for which one would expect to find supporting design documentation. In this method, the utility begins with the accident analyses identified in the FSAR. One utility program generated 18 analysis-based documents covering all FSAR accident analyses (see section 3.2(5) for more detail).

Utilities may find during review of source documents for their DBDs that few design documents exist for the plant. The plant design may be, for example, a takeoff from earlier plants of the same or similar design, and much information may be contained in correspondence with the attendant supporting calculations being those performed for another facility. There may arise a need to document engineering judgment and corporate memory of the NSSS vendor and the A/E in order to arrive at the basis for the design in some areas. In such cases, the calculations may be found to be confirmatory in that they may simply verify that a design used on a previous facility also was acceptable for use on the facility in question. For example, the volume of the reactor coolant system pressure relief tank may have been sized for one facility; however, for the second facility, the size may be based on the previous design except that the volume was increased by the ratio of the core thermal power. Facilities, therefore, may not have unique calculations or supporting design documents and the engineering design bases for one facility may reside in the engineering design bases of an earlier facility.

In the opinion of one utility, some of the open items and missing documentation are the result of a lack of documented systems integration by the original plant A/E. For example, structural calculations and analyses could not be found that related NSSS vendor design criteria to plant equipment specifications and parameters. The utility stated that it was able to find a substantial amount of detailed information, but the basis for the information or determination of design margins could not be traced. Calculations were found for system parameters, but the documentation was often informal and it was difficult to correlate the calculations with associated equipment. A portion of the engineering design-bases information that was found existed in teleconference notes, correspondence, and meeting minutes rather than in formal documents and reports.

For many of the older plants it is to be expected that much of the original design documentation does not exist, or may be difficult to retrieve at best. At the completion of a successful DDR program, a utility should possess sufficient design documentation, test data or substantiated and documented engineering judgments to demonstrate that the plant meets its engineering design bases.

As design calculations, analyses, or other design documents are retrieved from external design organizations such as the NSSS vendor or the A/E, utilities are assuming ownership of these documents within the bounds of proprietary information considerations. For proprietary information, the utilities will have a detailed knowledge of what information is available and where it resides.

Some utilities appeared to emphasize greater involvement of their design engineering personnel in the preparation of DBDs, even though all the utilities surveyed require varying degrees of outside assistance because of the large amount of data gathering, document research, and evaluation required for their programs. Other utilities subcontract virtually all of the effort required to produce and validate the DBDs and do not involve their design engineers significantly in the reconstitution process. For example, one utility surveyed produced high-quality system-level and topical DBDs, but the design personnel did not appear to use them since they were not involved in the development of the DBDs and were unfamiliar with the type of information they contained. The sense of ownership of the DBDs should provide an impetus to maintain the DBDs consistent with the current plant configuration.

3.1.5 Design-Bases Document Cross-Indexing to Design Documents

Design of modifications requires access to and understanding of all pertinent design information, which then forms the engineering design bases for the modification process. Therefore, the DBD is an important element of design control although not sufficient in itself. The utilities with DBD programs appear to share this opinion, their DBDs all contain some level of cross-reference to other design documents, such as calculations or analyses.

The utilities surveyed varied with regard to the depth of detail and cross-referencing of the DBDs to design input documents (such as the FSAR), to design process documents (such as system or component design calculations), and to design output documents (such as drawings and specifications). The degree to which operational documentation (such as operating and surveillance procedures) was referenced also varied among the six utilities. Several utilities had comparatively sparse references in the DBDs while others had a stand-alone index in each DBD to virtually all design-related documentation.

The former approach is manageable if some external, controlled, and comprehensive data base is maintained to support the more simplified DBD. The database would be the single point of entry into the design information. The latter approach has the advantage of providing a controlled, self-contained, single point of entry into the design information for a system or technical topic, but requires a more elaborate DBD.

Either approach may be workable, provided that the design engineer for a particular modification has a single point of entry into the design documentation and that all the necessary design-related documentation is linked for identification and access by the engineer. This access needs to be on a system or topical basis and needs to be comprehensive, tractable, and user friendly. Such design-related information includes, but is not necessarily limited to, accident and transient analyses, licensing commitments and requirements, design calculations, engineering evaluations, engineering procedures/standards, specifications, technical correspondence, configuration drawings, operating procedures, surveillance procedures, and plant modifications.

Most of the utilities provided cross-references within the DBDs for most if not all of these design-related documents, recognizing that all of these documents represent the plant's configuration with regard to the engineering design bases.

Finally, whatever methods are used to define, establish, and document design-bases information, an important attribute of the DBD and the configuration documentation is the ease by which the design engineer can determine the existing margins in the design as currently installed in the facility. A basic purpose of the DBD is to provide a tool for ensuring that design margins have not been exceeded. Design margins are discussed in detail in Section 2.4.7.

3.2 System-Level Design-Bases Documents

Most of the utilities surveyed are in the process of developing DBDs for key plant systems. Generally, the systems chosen for DBDs are those required for safe shutdown and accident mitigation. One utility considered expanding their program to include DBDs for systems that are not safety related but that can affect reliability. Because the approach to system-level DBD development is different at each of the utilities, direct comparison of the programs is difficult. Therefore, a synopsis of each utility's approach to system-level DBDs is given below.

(1) First Approach

One utility with a plant that recently began operation does not have a defined DBD reconstitution program. It believes that the quality and amount of design information obtained at the time of plant licensing from the A/E and the NSSS vendor, coupled with the cataloged and accessible information available through computerized design management and information systems, will enable its engineers to know what design documents are available, access these documents as required for the modification/design change program, and ensure configuration management requirements are maintained.

This utility contracted for a pilot program to develop system-oriented DBDs. The effort was not continued because the utility found the product to be more of an embellished system description rather than a engineering design-bases document. Although the amount of design documentation controlled by the utility is good, the true bases for plant safety systems may not be fully contained in that documentation. For example, many of the NSSS systems are extensions of earlier designs and the bases and justifications for these extrapolations may not be included in the documentation provided to the utility. This utility did think it would be beneficial to develop selected topical DBDs to address, for example, electrical separation and requirements to Appendix R of 10 CFR Part 50.

(2) Second Approach

Another utility with a recent vintage plant believes that DBDs are not required for engineering personnel. This utility has a configuration management enhancement program that is currently under way. It involves the preparation of equivalent DBDs for 86 systems and generic topics that were written for plant operations, maintenance, surveillance, and other plant groups. The documents were written to provide plant personnel with an understanding of the plant's design considerations and engineering design bases. The program should improve the plant organizations' understanding of the engineering design bases, why the engineering design bases must be maintained, and how plant actions could affect or compromise the engineering design bases.

An engineering design-bases document source reference guide was written that lists the sources of engineering design-bases information, how it may be accessed, how it may be used, and the limitations of its use. The guide is a controlled document, which allows it to be revised and upgraded as sources are changed or increased as a result of further development of the overall program. Plant system engineers are trained on the subject of engineering design-bases documentation and that training is extended to other plant groups. Existing design summary documents will be expanded to encompass and establish engineering design-bases information by codifying the system design information that currently exists in design documents such as drawings, calculations, specifications, procedures, and the updated FSAR. The design bases will be established for all safety-related systems, systems that can cause challenges of safety systems, and systems important to plant availability. The design bases will be established for the overall system and major components as a minimum and will envelop all features and components included in the plant surveillance program.

Three expanded system documents were drafted as a pilot program. The utility cited the following lessons learned from the pilot program:

- A sufficient level of engineering design-bases information existed in the engineering files.
- The enhanced document format was appropriate for presentation of system-level engineering design-bases information.
- Reviews by plant personnel were beneficial in creating a useful and complete document.
- The plant viewed the enhanced documents as beneficial to their programs.

- Several design and operations open items were found, but none required reportability in accordance with regulatory requirements.

(3) Third Approach

The remainder of the plants addressed in the survey have been in operation since the early to mid-1970's and their designs date to the late-1960's. One of these utilities initiated an enhanced DBD program to integrate the design requirements and design-related licensing commitments into a single document for each of the 37 systems in the program scope. Appropriate engineering design-bases information was included to support both safety and key operational functions and serve as an integral part of the overall configuration management program. The objectives of the program are to provide an effective and reliable source of engineering design-bases information; ensure the accuracy, reliability, consistency, and credibility of the available plant calculations; ensure the availability of documentation to support key design parameters; provide assurance that the licensing commitments are reflected in the enhanced DBDs; and ensure that key engineering requirements and assumptions critical to plant safety are identified in the enhanced documents.

Several types of documents have been researched as potential source documents for engineering design-bases information, including existing DBDs; analysis-based documents; calculations and analyses; plant licensing bases; NSSS vendor and A/E design criteria, standards, functional specifications and design reports; special project reports; NSSS vendor and A/E correspondence; plant modification packages; regulatory requirements and industry codes and standards; internal utility correspondence; design drawings; procurement requirements, outlines, and specifications; select vendor correspondence, drawings, manuals, and bulletins; pre-operational, startup and post-modification test reports; and plant procedures.

The utility developed several unique tools for the development of input to the enhanced DBDs. One of these tools is a set of logic trees that show the flow from general design criteria to safety function to system parameters and, finally, to component parameters for each safety function of the system. The trees enable the DBD preparer to focus on the important aspects of the system design and to determine the necessary information to support the engineering design-bases requirements. Another tool is composite safety function diagrams (success trees) that show the state (e.g., open, closed, running) of active and passive components necessary to complete specific system functions during various accident response modes.

The pilot program for two systems that the utility had completed showed that the enhanced DBDs had a unique and user-friendly format. System-level or component-level performance requirements that cover the spectrum of plant operation from normal operation to emergency operation are addressed. Automatic actuation and required operator actions also are addressed. The design and performance margins available for certain safety parameters are included, as well as why the margins were provided and limitations of the margins. The reason for both system and component performance requirements is given and the key source documents that contain the basis for the performance requirements are documented. The enhanced DBDs also contain interface requirements for support systems (such as heating, ventilation, and air conditioning; electrical power; cooling water; and instrument air) and indicate the system and component performance requirements that were or were not considered in the accident analyses.

The utility developed a program for the analysis-bases documents (ABDs) to complement the DBD effort. The utility contracted an NSSS vendor to generate 18 ABDs that covered all FSAR accident analyses. The ABDs document system and component operating parameters, briefly address analysis techniques, and identify the gross effect on the analysis if a parameter were to change. Since the reload analysis for the plant was done by the NSSS vendor, the document is most useful to the utility to conduct 10 CFR 50.59 evaluations. The ABDs also describe accident scenarios and contain assumptions made by the NSSS vendor in the accident analyses. The assumptions made in the ABDs were verified during plant walkdowns, and key parameters were validated where possible by reviewing startup test data (original plant startup and refueling outage startups), surveillance test results, and operating procedures. The field validations for the ABDs included operator actions assumed in the accident analysis that were determined by reference to emergency operating procedures. The ABDs were completed except for field verification activities at the time of the team's visit.

(4) Fourth Approach

Another utility with an older plant is in the process of preparing system DBDs for all of the plant systems that are required for safe shutdown and accident mitigation by (1) organizing, defining, and controlling the current engineering design bases and calculations of record, (2) validating the critical design parameters related to the plant procedures and hardware against the regenerated or current engineering design bases, and (3) creating and maintaining an experienced knowledge base within the utility.

Each of the 22 system DBDs will incorporate, either directly or by reference, the system's engineering design bases, the system calculations, analyses of record, and the system-descriptive design documents. The utility considers the system engineering design bases will be accumulated from the NSSS-imposed system functional requirements, the regulatory-imposed design requirements, and the design codes and standards of record. The system calculations and analyses of record are contained in design documents such as accident analyses, component sizing calculations, and piping stress analyses. Examples of system-descriptive design documents are component specifications, general arrangement drawings, flow diagrams, purchase orders and other procurement documents, vendor manuals, FSAR, technical specifications, testing procedures, and installation procedures.

The system DBDs are intended to enable the utility's engineering group to prepare design modifications to plant systems in a consistent and timely fashion and to enable the plant system engineers to validate the performance of each system with regard to the system's functional requirements detailed in each DBD. The design requirements for the major components within each system also will be specified.

The utility has generated and issued three system DBDs developed as part of a pilot program. The pilot program has discovered only minor discrepancies for the systems designed by the NSSS vendor. The utility anticipates substantially more discrepancies will be discovered with the systems designed by the A/E and others because of the interface requirements and the looser control of quality records during the timeframe in which the plant was constructed.

(5) Fifth Approach

A fifth utility, which also has an older plant, has completed development of DBDs for 18 key accident mitigation and support systems. Two documents, one on a system-level basis and the other on a component-level basis, capture the basic functions, performance requirements, and interface requirements for each system and component. Several of the system-level documents contain an adequate level of information for the functional bases of the system that is well supported by reference to supporting documents and calculations. For some systems, detailed flow, heat balance, or other calculations were performed to validate the capability of the systems to meet design requirements because of technical issues that arose during the reconstitution process.

(6) Sixth Approach

The sixth utility, another older plant, is well under way in its DBD reconstitution program and has defined 35 system-level DBDs to be developed. An interesting feature of the program is the development of design-bases documents for the auxiliary building, the containment, the intake structure, and the security building. The development of the DBDs are controlled by a writers' guide and a detailed development guide.

The selection process for the generation of system DBDs is based on the importance of the system to nuclear safety, the frequency of modifications to the system, the complexity of the system, and the importance of the system to sustained plant operation.

The information contained in several of the DBDs was comprehensive and useful without being overwhelming. The intention of this utility was to make the DBDs a directory for easy access to detailed engineering design-bases information. It did not want the DBDs to become documents of only academic interest or documents that are subject to constant change as modifications are made to plant systems. The utility used one DBD to resolve conflicting information concerning the qualification level of a component.

Several weaknesses were evident in the DDR programs of the utilities surveyed. One program tended to contain a significant amount of descriptive material rather than being focused on the design intent and providing references to specific engineering design-bases information. Another program was inconsistent in the format, type, and level of information contained in the documents as a result of a writers guide that allowed too much flexibility in the development of the documents. Sections of the documents on design margin addressed only FSAR-type margins and did not address design and performance margins available in system and component designs. Another program provided engineering design-bases information that was derived from procurement specifications rather than information that reflected the true engineering design-bases requirements. In addition, the information was not verified or validated, which made it suspect. The two major programmatic weaknesses were the lack of emphasis placed on the verification and validation of DBDs and the lack of a methodology to assess the necessity and timing to regenerate missing design documents.

The content and format of system-oriented DBDs varied in the level of detail and arrangement of information, but the categories of information were similar. A number of fundamental and notable attributes resulting from the survey team's review of industry DBDs were identified that may be useful to utilities that are planning a DBD program or are in the process of initiating one (see Appendix F).

3.3 Topical Design-Bases Documents

A number of the utilities surveyed have developed or plan to develop generic or topical documents for issues that are common to many plant systems and areas and are important engineering design bases to consider in modifications and maintenance of plant design. One utility included such topics as general design criteria, seismic criteria, tornado missile criteria, pipe break criteria, safe shutdown criteria, electrical separation criteria, external environmental criteria, internal and external flooding criteria, control of heavy loads, single-failure criteria, fire protection criteria, internal missile criteria, regulatory guide compliance, and environmental qualification. Other utilities included in their generic documents such topics as site meteorology, welding, accident analyses, emergency facilities, hardware and instrument installation, personnel protection, records retention, instrument classification, and seismic events. One utility included generic design issues in subsections of their enhanced DBDs and does not intend to develop separate generic documents for the topical issues. The utilities did not intend to validate the implementation of design attributes covered in topical DBDs.

The development of generic or topical documents would provide a concise and comprehensive design guide for use by the contracting organizations developing the major design modifications for the plant. These documents also would provide the utility's corporate engineers with rapid and comprehensive access to detailed topical design information, to enable spot checks of the design modification packages. In addition, a verification and validation process applied to the attributes addressed by the generic topics would enhance DDR programs.

3.4 Level of Effort

The utilities with formal DDR programs have expended a great deal of staff and financial resources on their programs. Personnel from the utilities and in the support organizations, such as NSSS vendors, A/Es, and other contractors, are dedicated to the DDR task. These personnel retrieved plant design records from archives, reviewed the documentation to find those dealing with engineering design-bases information, compiled the information into the DBDs, produced and reviewed the documents, and performed verification and field validation of the information contained in the documents. One utility estimated that each document of the ones planned would require 1500 staff hours to prepare and cost approximately $300,000, including field validation and regeneration of missing calculations required to validate key functional parameters.

A typical retrieval effort involves identifying, collecting, indexing and organizing all applicable records needed for the input to DBDs. Records are located in NSSS vendor and A/E files, various utility files, engineers personal files, and local warehouses. Licensing correspondence and the original FSAR and NRC safety evaluation reports also are a source of engineering design-bases information. One utility's task was complicated since the original plant A/E closed its local office and later was absorbed by another company on a corporate level. Other difficulties arose as a result of certain information being designated as proprietary by the NSSS vendor or others. Over one million documents may be screened for engineering design-bases information for a particular plant, but the number of documents with pertinent information is usually substantially less. Documents obtained through the screening process are usually loaded in a computer data base for later search and retrieval efforts during the DBD writing effort.

The organizations that prepare the DBDs are usually contractor organizations, plant A/Es, or NSSS vendors. The utilities provide program management and establish the writers' guide that delineates the format and content of the DBDs and the level of detail to be contained in them. The utility control exercised during this process varies from directly involved to program oversight. However, those utilities exercising tighter control and leadership in their DBD reconstitution programs have the better and more useful documents.

The better utility DDR programs include verification of the information contained in the DBDs with the source documents and other confirmatory documents. Most programs also include field validation of the information to ensure consistency between the DBDs and the physical configuration of the plant. The more aggressive validation process often includes a safety system functional inspection (SSFI) of several systems in addition to plant walkdowns and physical confirmation of the system against the design basis. One utility intends to perform an equivalent SSFI on each of the systems included in its program. This type of engineering inspection is the way in which the NRC has checked the adequacy of the results of design control and DDR programs.

3.5 Priority for Design-Document Regeneration

The DBDs generally are prepared in accordance with a priority that considers the safety significance of the system, the frequency of modifications to the system, the complexity of the system, the importance of the system to sustained plant operation, the possible effect of the system on safety-related systems, the importance of the system to environmental qualification, and safety-related topical design considerations. An overall list of the systems, structures, and topical DBDs that the utilities have prepared or plan to prepare is provided in Appendix G. Several of the plant programs represent enhancements of previously developed DBD-type documents. The number of DBDs to be issued ranged from 18 to 84. The programs reviewed by the team are scheduled for completion before 1993.

Some utilities had informal methods for determining the necessity and timeframe for document regeneration. These determinations were in large measure made on a case-by-case basis, based on the judgment of the cognizant discipline lead engineer. Other utilities just identified the documents as missing, delaying evaluations and decisions on reconstitution until later in the program. Most utilities are considering regenerating only missing design documents that are required to validate critical system or component functional attributes, especially if these resulted in a reportable item. Missing documents are usually identified during the preparation and field validation of the DBDs.

Prioritization for the regeneration of less critical but important design documents is generally lacking. For example, whereas a missing calculation for system net positive suction head may be regenerated, regeneration of missing seismic qualification documents is not planned, particularly if archived correspondence indicates that such seismic qualification was originally performed. As a consequence, a number of system and component seismic qualification requirements and attributes may not be confirmed.

One utility had an elaborate categorization program for open items found during the DBD development program. Categories exist for missing or conflicting documentation or other concerns that are not reportable under NRC notification regulations, but are important to the engineering design basis of the plant. While reconstitution is in order for these items, the priority and timeframe for reconstitution has not been established.

During the early stages of the DDR process, utilities found that many unanswered technical questions arose involving potential nuclear safety issues and deviations from NRC requirements that could not be readily answered. These questions arose because of undocumented design bases, calculations, and analyses; documentation conflicts; or undocumented verification. The questions were dealt with on a priority basis and, on several occasions, led to a plant shutdown while the issue was resolved or to an extensive effort expended on a priority basis to demonstrate that the facility was being operated within its design bases. The utilities soon found that the number of questions outstripped the capability to address each one on a priority basis. As a result, to prioritize and resolve questions based on the safety significance of the question, several utilities have used or are planning to use probabilistic risk assessment techniques. Questions with high safety significance are given priority evaluations, while those judged to be of moderate safety significance are given a more routine evaluation.

One utility employed a risk-based prioritization using standard reliability techniques. Available data bases are used as a screening tool. The risk screening process identifies the failure of concern, the consequence of concern, the time sequence of concern, the time sequence of events, and quantifies the limiting scenario. Risk categories are developed based on the probability of the scenario compared to risk values of core melt (1E-4) or severe release (1E-6). The results are further screened against NRC requirements and the contribution of the subject scenario to the cumulative risk of all assessed risk items to come up with a resolution category. Thus, a scenario with a very low risk, which made it a low priority item, could still result in a plant shutdown categorization because of a violation of NRC requirements.

This utility realized the benefits of integrating design, operations, and risk perspectives and enhancing understanding of plant safety as an ordered approach to resolution of technical issues. This utility had a unique approach for the reconstitution of missing design analyses. Rather than regenerate individual missing design calculations, the utility developed detailed thermal-hydraulic analytical models of plant fluid systems to determine whether they would be able to perform their intended design function. In developing these models, several design concerns were discovered that were categorized as potential high-risk issues. The utility recently extended the program to include any unconfirmed technical issue that is identified for its nuclear plants.

3.6 A/E and NSSS Vendor Involvement

The roles of the original plant A/E, the NSSS supplier, and other contracting organizations in the preparation, review, and validation of plant DBDs vary throughout the utilities. One utility has a well-developed in-house engineering capability and is in the process of preparing its own DBDs. The utility purchased all of the design records that the original plant A/E could access and interfaced with the A/E on a limited basis to interpret these design records. The utility also contracted with the NSSS supplier to prepare design-summary documents (through the operational licensing timeframe) for the systems that the NSSS supplier designed in whole or in part. The utility incorporated the information from these design-summary documents into the system DBDs. Except for these external interfaces, the utility's engineering and plant staff are preparing, reviewing, and validating all of the plant's DBDs.

Another utility was the A/E for its plant, but plans to use other A/Es and consultants as necessary to assist in the preparation of enhanced DBD-type documents. This utility also retained the NSSS supplier to review and approve the documents that have been prepared for the plant's NSSS systems. It has developed a writers' guide for the enhancement program.

Another utility has accessed all of the design records that the original plant A/E had archived. However, since another A/E has prepared plant design modifications and performed design services for the utility over the past 12 years, the utility chose the latter A/E to conduct the DDR effort because of its familiarity with the plant's design. The work effort and resultant product has been tightly controlled because the A/E is working as an extension of the utility under the utility's program procedures. To obtain NSSS design information, the utility has joined with other utilities in an owners group to collect and index NSSS design information from the NSSS supplier. This task is expected to be completed in mid-1990. The NSSS supplier also is preparing several DBDs for this utility's NSSS systems. The A/E has developed a comprehensive set of procedures to control the DDR project in accordance with the utility's procedures and program. While the A/E is preparing the bulk of the remaining DBDs, the utility has prepared several DBDs in-house.

Another utility continues to rely heavily on the original plant A/E, NSSS supplier, and other contracting organizations to perform design modifications to its plant. These organizations maintain many of the plant's original design documents for the utility. However, this utility has prepared DBDs in-house and has used the plant A/E and the NSSS supplier primarily to provide the calculations and other design documents that the utility required to prepare the DBDs. To assist the utility in the preparation of the DBDs for the plant's NSSS systems, the NSSS vendor has prepared nonproprietary versions of the design information for each NSSS system. Supporting calculations and other design documents are available in a proprietary library maintained by the vendor in a local office near the utility headquarters.

The remaining utility continues to rely heavily on the original plant A/E, the NSSS supplier, and other A/Es to perform design modifications to its plant. These organizations continue to maintain many of the plant's original design documents for the utility. The utility had contracted with the plant A/E and the NSSS supplier to prepare and validate the DBDs in accordance with the utility's quality assurance programs and writers' guide.

The NSSS vendor surveyed stated a concern that many utilities perceive the NSSS design interface package provided at commercial turnover to be design-bases information when, in fact, it is predominantly design-configuration information. The vendor's implicit definition of design documents are those documents that ensure that the NSSS vendor can supply an identical or equivalent replacement for any piece of equipment that has been in the original NSSS scope of supply. The bases for the configuration so described may not have been included in these design documents. The vendor stated that much of the NSSS engineering design bases are contained in test program results rather than in calculations. The opposite situation was generally true with A/E design information.

The NSSS vendor noted that newer plants have as much need for engineering design-bases documentation as older plants because the fundamental engineering design bases for important aspects of recent designs are often established in earlier design evolutions when documentation requirements were much less rigorous.

The vendor favors the early establishment of a DDR team consisting of the NSSS vendor, A/E, and the utility. It favors beginning with DDR pilot programs for one or two systems and emphasizes the ownership of the DBD by the utility. The vendor observed that utilities with organizations that are strictly discipline-oriented have more problems understanding engineering design-bases requirements than utilities that have system engineers within their design organization.

The NSSS vendor has not encountered major problems with document retrieval for the DBD programs it has supported to date. Design requirements at the start of commercial operation are easily retrieved. Recovery of engineering design-bases information may consist of written documentation of the bases or a consensus opinion of design personnel who were involved during the original design. If the consensus approach is used, the information would be documented and filed for future reference.

The NSSS vendor estimated that preparation of a DBD for a system originally within their scope of supply would require about 3 to 4 months of effort because the number of senior people still actively employed and available to support a given NSSS system are limited. A utility DBD program having a 3- to 5-year duration generally can be supported. The vendor cautioned that the utilities should act while the experienced engineers that were actively involved in the projects during the design and construction are still available.

3.7 Verification and Configuration Validation

3.7.1 Verification and Validation Overview

The scope of the process used by most of the utilities surveyed to ensure that a DBD is correct and that the plant configuration conforms to the DBD is similar to the following definition from ANSI N45.2.10:

> Verification: An act of confirming, substantiating, and assuring that an activity or condition has been implemented in conformance with the specified requirements.

Other useful definitions for verification and validation have evolved in the design practice for digital systems. A distinction is made between verification and validation (see Electric Power Research Institute document NSAC-39, "Verification and Validation for Safety Parameter Display Systems," and Institute of Electrical and Electronic Engineers [IEEE] Std 729-1983, "Software Engineering Terminology"):

> Verification is the review of the requirements to assure the correct problem is being solved, followed by review of the design to assure the requirements are met. The verification activities apply to the translation of design information from one development phase to the next, and involve document checking/review at each successive design phase, with testing used as practical. Validation is the test and evaluation of the integrated system to determine compliance to the functional, performance, and interface requirements. Therefore, validation provides an overall assurance that the capabilities specified in the system requirements have been implemented in the design.

While the ANSI N45.2.11 definition of verification appears to encompass both verification and validation, for the purposes of this report the team preferred to define the terms separately. That is, DBD verification is defined as the process of checking that the information contained in DBDs has been correctly and consistently translated from the source documents. Validation, or field validation, is the process of ensuring that the physical plant and the DBDs are consistent and that system configuration and functionality is accurately represented by the utility design documents. Validation also includes checking that the information contained in other plant documents, such as operations, maintenance, and surveillance test procedures and vendor manuals, is consistent with the information in the DBDs.

The use of these definitions does not imply that a rigorous check is required of previously approved design documentation. A reasonable approach would be to verify that the design documentation retrieved, particularly documentation that was generated during the initial design phase, is consistent with the current plant configuration. Review of existing calculations for technical adequacy, accuracy, and degree of representation of the current as-built configuration is not part of most of the utilities' DDR programs except where SSFI techniques are used in the validation process. Checking calculations would be appropriate where requirements have changed or where essential missing information requires regeneration of documents. Also, controls should be established to protect the integrity of source data and its accurate translation into the DBD.

DBD attributes concerning system functional configuration, performance, or operation are generally selected for validation. In some instances, critical component functional parameters such as flow rate, heat transfer, response time, and temperature also are selected for validation. Topical DBDs covering design considerations such as seismic design, missile protection, flooding, and other topical engineering design bases generally are not selected for validation. Where these requirements have been addressed in other programs, such as the program in response to IE Bulletin 79-14, "Seismic Analysis for As-Built Safety-Related Piping Systems," further validation is sometimes not performed by utilities.

Some level of validation of the plant configuration with the DBD is needed to ensure that modifications have not created a condition beyond the design bases and to ensure that correct design margins have been established for consideration in future modifications. A comprehensive validation program typically will address functional, performance, and interface requirements established in the DBD. Validation tools for achieving this purpose include reviews and walk-throughs of configuration drawings and documents; physical walkdowns of plant hardware; reviews of existing calculations; performance of confirmatory calculations; reviews of preoperational and surveillance test results; reviews of actual plant transient responses; performance of confirmatory tests; references to existing confirmatory programs (e.g., Appendix R to 10 CFR Part 50; NUREG-0737, "Clarification of TMI Action Plan Requirements," November 1980; 10 CFR 50.49; and Bulletin 79-14 programs); reviews of modification packages/safety evaluations; sampling programs for generic topics (e.g., anchorage calculations, electrical separation, and modification packages); and performance of select internal SSFIs.

As a part of a validation program, it is generally recognized that certain design documents and implementation of certain engineering design bases are more likely to contain discrepancies than others. However, the areas of emphasis to some extent depend on the age of the facility and the effectiveness of previous utility design-control programs and practices. By intelligently selecting a sample of the engineering products for verification and/or validation, the utilities could maximize the safety benefits obtained for the resources expended. For example, it may be beneficial for early vintage plants to place additional emphasis on the calculations and design documents that were performed before the implementation of 10 CFR Part 50, Appendix B. It also may be beneficial to place additional emphasis on validating the implementation of design bases such as physical and electrical separation. These design requirements were imposed by NRC at a time when the designs of some facilities were in progress. The requirements to harden facilities against high-energy line break, natural phenomena (e.g., seismic events and tornadoes), fire, and internally generated plant missiles may not have been as rigorously addressed in older facilities. In some cases, the facility designs may have progressed to quite an advanced stage and required innovative re-engineering or relocation of installed hardware and components. Further, it may be more cost effective for a utility to target systems that have been modified many times by many organizations for an internal SSFI. The NRC has used this technique to judge the effectiveness of DDR programs. Conversely, plants that have undergone integrated design inspections or independent design verification programs as a part of the licensing process may decide that less scrutiny is necessary for aspects of the facility that were previously reviewed, particularly if they have not been modified. Since design control has improved over the past few years, it may also be beneficial to scrutinize older modifications, perhaps implemented under less stringent design control practices, to ensure engineering design and licensing bases were not compromised.

3.7.2 Utility Verification and Validation Programs

Most utilities appeared to verify DBD source documentation with the support of the original NSSS vendor or the original A/E. Verification generally consists of retrieval of hardcopy evidence of the design-basis information or a documented consensus of available experts if existing documents are not retrievable or evident. The translation and compilation of these source document requirements into the DBD is a procedurally controlled process.

With one exception, the utilities surveyed appeared not to significantly challenge existing DBD source documentation. For example, most appeared to simply accept the existence of a calculation rather than verify its assumptions or methodology. One utility appeared more aggressive in this regard, although the utility did not have a large technical staff, it appeared more effective in assuring that the DBDs were accurate and complete. For example, the utility used data from abnormal operating events, such as a lightning-induced loss of offsite power, to verify assumptions made in the DBD source-document analyses.

All of the utilities use design configuration validation tools described previously. However, a wide range of difference was observed among the individual utilities' scope of validation and emphasis.

The utility that appeared to have the most aggressive DBD verification program also appeared to have a very effective configuration validation program for system design. The utility uses the following guideline to determine which engineering design-bases attributes require field validation: a parameter that requires validation is (1) derived from or based on a licensing commitment, (2) essential to the performance of the safety function or component, (3) a calculation assumption or specified in NSSS vendor or A/E correspondence and not likely to be well known or understood by engineering or licensing personnel, and (4) significant as determined by operations or the PRA group. The utility performed field validation of critical calculations, which were based on the assumptions of normal and accident conditions, to demonstrate that (1) the systems are capable of performing the safety functions required by their engineering design bases through appropriate physical walkdowns, (2) testing is adequate to demonstrate that the systems would perform all of the safety functions required, (3) system maintenance (with emphasis on pumps and valves) is adequate to ensure system operability under postulated accident conditions, (4) operator and maintenance technician training is adequate to ensure proper operations and maintenance of the system, (5) human factors considerations relating to the selected systems (e.g., accessibility and labeling of valves) and the systems supporting procedures are adequate to ensure proper system operation.

However, some of the utilities surveyed have validation programs that lack sufficient attention to topical DBD areas such as single failure, system interaction, seismic design and separation requirements. Others have inadequate validation of component-level design requirements and information contained in the DBDs, and other utilities focus on design-related weaknesses in plant procedures rather than including design documentation.

3.8 Operability and Reportability

Utilities were concerned about the questions of operability and reportability that could arise from DDR programs. For example, utilities were unclear if systems, structures, and components should be considered inoperable if documentation that provided assurance that the plant was being operated within its design bases was unretrievable. Some plants had needlessly been shut down or had reduced power as a result of documentation problems. In addition, there was the potential for generating a substantial number of reportable events, many of which would later be determined to have been unnecessary. (Additional insights into these questions can be found in the Nuclear Management and Resources Council's (NUMARC's) "Design Basis Program Guidelines" document dated October 1990.)

There is a clear linkage between operability and reportability determinations. Once the determination has been made that the facility has been or is operating outside its design bases or that systems, structures, and components may be incapable of performing their intended safety function requirements for reportability as specified in 10 CFR 50.72 and 10 CFR 50.73 become operative and the time clock starts for any affected action statements as defined in the facility's technical specifications. These operability and reportability judgments are of particular concern during the DDR phase for older plants designed before the existence of Appendix B to 10 CFR Part 50 and NRC endorsement of ANSI Standards N45.2.11-1974 and N45.2.9-1974 as requirements for design documents and record retention. Design documentation practice for the older plants was not as rigorous as more recent practice so that missing or incomplete documentation is not unusual and is not necessarily an indication of an inadequate design or other immediate safety concern.

4 CONCLUSIONS AND OBSERVATIONS

It is very difficult to characterize the performance of nuclear utilities in the area of design control and configuration management on the basis of a rather limited survey of six licensees and one NSSS vendor. The one thing the survey team can conclude with a high degree of confidence is that each utility controls design and approaches configuration management in a different manner. Certainly, there are similarities in the programs of different utilities by virtue of the fact that they are all, in their own way, trying to achieve many of the same goals and objectives. However, differences in organizational structure and areas of emphasis result in different approaches.

In developing its conclusions, the team drew from the strengths and weaknesses they perceived during the survey of the approaches and programs of the various utilities. Utility programs may have evolved since the survey was completed; therefore, the team's conclusions should not be interpreted as being critical of, or an endorsement of, any current utility approach or program. Additionally, for completeness, the survey team has drawn from its direct knowledge of program strengths, weaknesses, and problems encountered by utilities that were not part of the survey. Therefore, the conclusions and observations given below should be viewed as a global account of the organizational or programmatic attributes that have been beneficial or have caused problems in design control or design-document reconstitution.

4.1 Overall Assessment of Utility Design Control

4.1.1 Engineering Capability

The utilities surveyed had adequate procedures and practices to control the interface between the corporate and site engineering staffs. While each organizational structure had its strengths and weaknesses, in most cases, where the engineering organization had the responsibility to control the plant design, configuration, and modifications, the design documentation was more complete and there was less likelihood that temporary and permanent plant modifications abrogated the plant's design and licensing bases.

The utilities with plants that had recently started up had larger design staffs with more engineering disciplines and performed more fundamental design engineering in-house. Utilities with plants that had started up in the early to mid-1970's tended to have smaller staffs and relied more heavily on outside contractor organizations for the more complex and involved design activities while overseeing these activities in a project management role. Although operating in a project management role is one of several ways for the utilities to control and implement plant modifications, it is still imperative that the project management staff be sufficiently knowledgeable to be able to ask the right questions of the organization or person performing the work. This is true even for the more arcane technical specialties (e.g., seismic analysis or reactor core thermal/hydraulic analysis) for which it may not be justifiable to retain in-house capability. However, the team observed that project management staffs were not always sufficiently knowledgeable. Although, of necessity, some percentage of engineering work must be performed by contract organizations, it is the licensee's responsibility to ensure that the work is done correctly and that the plant remains within its design bases. It is important for utilities who have delegated design responsibilities to outside contractor organizations to establish engineering assurance programs and to maintain active technical management involvement and control of the design process. This is necessary to ensure consistency in the design control process and to maintain control of the configuration management program.

The percentage of engineering work done in-house varied among the utilities surveyed. The utilities that retained a solid in-house engineering capability tended to have a more thorough understanding of their engineering design bases and current licensing bases and of the implementation of these bases. If a significant portion (40 to 50 percent) of engineered plant modifications (complex as well as simple modifications) were done in-house, the utility would maintain a technically competent engineering staff that was in touch with the current technology.

There was a lack of utility design procedures (in-house design guides and procedures) and the utilities tended to rely heavily on industry consensus standards to engineer modifications. Certainly consensus standards are necessary and useful, however, they are typically broad-based documents that permit multiple ways to achieve an acceptable design. The development and use of in-house design guides would further refine and provide for a more consistent design approach to the implementation of the guidance provided by consensus documents. The use of in-house design guides would help to ensure that the engineering design bases are considered in developing plant modifications. These documents could also standardize, to the extent possible, the manner in which commitments in the plant's design bases are implemented.

An important part of the design control, and also the design reconstitution process, is the recognition (but not necessarily quantification) of where design margins exist and their categorization as being controlled by the design organization or by the NRC.

It may be beneficial to quantify and control design margins when they are referenced as the bases for acceptability of a design modification or a modification to plant operating procedures. Original margins tend to be slowly consumed during the life of a facility by various modifications. Many Class 1E electrical systems, for example, had excess capacity when the facility began commercial operation. Over the years, electrical loads were continually added to the Class 1E system by designers, secure in the knowledge that ample margin existed, only to realize one day that the margin they thought existed had been consumed and, in fact, the diesel generators were unknowingly being required to operate in a condition in excess of the manufacturers continuous-duty rating.

The identification, definition, categorization, and tracking of margins in the original plant design and during the design change process was generally weak.

None of the utilities had thoroughly kept track of design margins, nor considered how small incremental changes to systems could affect design margins. Many utilities did not update controlled calculations to incorporate minor changes or track these minor changes so that they could be assessed in aggregate to determine the total effect on system or component performance. Utility engineers relied on undocumented engineering judgment to assess the effect of small changes on system performance. Although the use of properly documented engineering judgment is a valid way of assessing the effect of incremental changes, if the incremental changes are not tracked and the decrease in available design margins are not documented, at least qualitatively, sooner or later the design margin will be nonexistent and systems may no longer be able to perform their intended safety functions. If utilities developed and implemented procedures and controls to track incremental changes to design calculations, the control of design margins would be enhanced.

In addition, although documented engineering judgment can be relied on to determine the threshold for revising the calculations for consideration of the aggregate effect of the design changes, it is important that the related history of a calculation remain with the analysis of record. There were instances where the rationale for these engineering judgments was contained with the modification packages and not with the original calculations. Therefore, an engineer subsequently modifying a system would have to retrieve all the previous, related modification packages to understand where margins may have been reduced from the original design. It would be beneficial if all original design calculations and design-change-related calculations--performed by either the utility or by A/Es, NSSS vendors, and other contractors for the utility--were logged and filed in utility document-control systems independent of the associated design-change packages. In this manner, calculations would all be recorded in a central location and an engineer would be able to review a list of calculations for a particular structure, system, or component to determine if reanalysis had been performed and if the original design analysis was still valid and remained the analysis of record. Where calculations are restricted because of proprietary considerations by outside companies, it would be useful if utilities had summaries and listings of such calculations in their files.

All the utilities surveyed had adequate methods to identify and to control in-progress modifications so that other engineers and designers would be aware of planned but perhaps not yet implemented modifications that could affect the modification on which they were working. However, all utilities should pay particular attention to their design-change control procedures and implementation programs to ensure that controls are established to minimize the occurrence of conflicts or adverse interactions between simultaneously ongoing modifications. It is important that procedures also ensure that partial implementation of a modification does not result in a condition that lies outside the approved system design.

Most utilities have adopted the systems engineer concept. The adoption of the systems engineer concept is indicative of a proactive utility organization recognizing the need for this coordination/interface function. Extending this concept to the design organization also would be beneficial because in many instances there is no system ownership in the engineering organization and any one of several individuals may prepare modifications for any given system. Therefore, it is not likely that any one engineer in the design organization fully understands the engineering design bases of a given system or what prompted certain decisions to be made and why and how certain design considerations were implemented. Extending the concept of the systems engineer to the design organization would add greater depth of knowledge to the design organization as well as create a single point of contact or design counterpart to the systems engineer on site. It would also establish a cognizant individual for specific system or topical DBDs that would be created by a utility DDR program. The systems engineer in the design organization could have responsibility for maintaining his/her assigned DBDs current and assuring that his/her assigned system remains within its engineering design bases.

In several of the utilities surveyed, the responsibility for instrumentation and control (I&C) was under the electrical power discipline, which appeared to dilute the resources available to handle modifications in the I&C area. Considering the rapid change in technology in the I&C discipline (e.g., the use of digital instrumentation systems in place of analog systems, the increased use of fiber optics, multiplexing, and computerized protection systems with safety-related software), a dedicated organization to handle I&C modifications could be beneficial. Additionally, having designated individuals controlling the probabilistic risk assessment and the failure modes and effects analyses also is worthy of consideration.

The computer-based, fully integrated, configuration management information system under development at one utility appeared to be a very capable and useful tool to retrieve design information. In-house development of the software for the system and the close working relationship between corporate computer programming experts and configuration management personnel appeared to be a key factor in the successful development of such a system. In the future, systems such as this will help to ensure consistency of design inputs when design changes are made.

4.1.2 Control of Plant Modifications

There appeared to be appropriate lines of communication between engineering, groups responsible for implementing plant modifications, and operations personnel.

The development of a facility modification is a complex process that requires not only coordination of the various engineering design disciplines but also coordination between the engineering and site personnel.

A comprehensive design considerations checklist, which identifies appropriate design inputs, design attributes, design criteria, and design documents, is a useful tool for the design engineer. Further, multidiscipline walkdowns before engineering the complex modifications were beneficial to identify and perhaps resolve questions regarding interferences, operational problems, sequence of installation, and other synergistic design considerations. Periodic multidiscipline meetings held before and during the implementation of complex modifications were beneficial for planning the work in advance, defining organizational responsibilities, and resolving any problems that arise.

Utilities should encourage walkdowns before, during, and after a modification is installed, particularly for complex modifications. The walkdowns would be most beneficial if they were performed by a team comprised of design, construction, operations, maintenance, systems engineers, and health physics personnel using a standard set of questions. Walkdown observations and discrepancies could be jointly resolved by the participants. Following modification implementation, a formal walkdown involving the systems engineer, the design engineer, and representatives of other organizations such as the installing organization, operations, maintenance, and the QA/QC organizations should be held to ensure proper implementation of modification details.

The procedural requirements for system turnover of modifications were thorough at most utilities. It is very important that drawings and procedures critical to system operation, such as those identified below, are updated in the control room before modification turnover to operations.

- drawings such as P&IDs, electrical single-line diagrams, schematics and logic diagrams, and valve and instrument lists
- technical manuals required by operations
- operating procedures
- emergency operating procedures
- set point documents
- surveillance test procedures required for operability determinations of the modified system or equipment
- electrical load list for Class 1E busses

4.2 Assessment of Utility-Initiated Design-Document Reconstitution Programs

4.2.1 Development of Design-Bases Documents

Each utility surveyed had evaluated the need for a design-document reconstitution program and proceeded according to its needs. Each utility operates differently, has a different organizational structure, and perhaps has facilities of different ages with varying degrees of available documentation; therefore, each utility must review its needs, establish the goals it wants to achieve, target the primary users of the products, and develop a program that fulfills its objectives. Accordingly, it follows that each facility should have its own program. Even within the same utility, where facilities of different vintages may exist, it is not unreasonable to expect to have somewhat different programs for each facility. It follows that the format and content of the DBDs for each facility may be unique since they are driven by the predefined programmatic goals and objectives and the needs of the end users. However, since most utilities have common objectives, many DBDs may contain similar types of information. Appendix F provides a listing of fundamental design-bases document attributes.

DBDs are beneficial because they can capture the current corporate memory of the engineering design bases (including the NSSS scope), the design decisions that were made, and the rationale behind these decisions. Experience has shown that this information held in corporate memory fades over the years as a result of staff turnover and attrition. DBDs also provide a user-friendly, central location for the engineering design bases and current licensing bases and a directory to supporting design documents. DBDs, for example, can provide reference information to support 10 CFR 50.59 evaluations necessary for temporary modifications or regulatory waivers of compliance that may be required on an expedited basis to keep a facility operating. Such situations regularly arise at inopportune times, such as during weekends or on backshifts, when perhaps the individuals most knowledgeable of the specific design considerations in question or design margins available are not on site or readily reachable.

Utilities may find it a worthwhile exercise to evaluate their organizations to determine the need for implementing some form of DDR program on the basis of the following factors: (1) loss of engineering and design corporate memory (i.e., utility, NSSS vendor, A/E) through personnel attrition, (2) the normal evolution of the utility organization from a design to an operating orientation with the typical shift in priorities away from expending resources to maintain and update design documents, (3) lack of a centralized design engineering organization with responsibility for design control and configuration management shifted to the operating organization, (4) extensive reliance on contracted engineering services with minimal licensee capability to provide technical oversight, (5) the availability of design bases and design analyses and calculations to support the as-built plant, and (6) the ability to make timely operability determinations. (Further self-assessment questions are addressed in Appendix H.) On the completion of such a self-assessment, utility management could judge whether a DDR program would significantly enhance their level of knowledge of the plant design and the accessibility of information. If a decision was made to initiate a DDR program, the self-assessment could provide the bases for developing the goals and objectives of the program.

If a utility decides to initiate a DDR program, it should recognize that implicit in this decision is a commitment of the necessary personnel resources and management oversight to ensure management goals and objectives are met and that the program will produce documents that may be effectively used in design control, configuration management, and plant operational programs.

However, the commitment of utility personnel to produce a useful set of quality documents is an important ingredient to the success of a DDR program for several reasons. First, the task of putting together a DBD will provide the individuals involved with a wealth of information about and insights into the systems engineering design bases and with the reasons why certain design decisions were made. It seems prudent to keep this knowledge in-house. This can be better accomplished if the DBDs are developed by utility personnel rather than contractors. Second, utility participation provides a strong sense of ownership of the DBDs and a greater appreciation and understanding of the information contained within the documents and of the amount of effort necessary to compile the information.

Strong participation of the utility staff in the development of the DBDs should be encouraged by utility management to yield an increased appreciation of the plant design bases and to result in a greater level of acceptance of the DBD documents by the working-level utility staff. The best way to achieve an immediate level of engineering involvement is to dedicate utility design engineers and appropriate plant personnel to the DDR program and to maintain the DBDs as living and useful documents in the modification programs. However, it is necessary for the utility to do more than assign or contract a group to develop, compile, and distribute the DBDs to well-defined users. It is also necessary for the utility to develop an awareness and understanding of the plant's design bases and its importance within engineering and plant organizations. The DBDs can be useful toward this end, but are not a substitute for utility engineering involvement in the design of facility modifications.

At the conclusion of a DDR program, most utilities have a thorough understanding of their engineering design bases, a sufficiently complete set of documents that demonstrate how the engineering design bases were implemented, and a high level of confidence that the current facility configuration is consistent with the design documents and is being operated within its design bases.

The level of involvement of the utility's design organization in the DDR process is a major factor in the quality and usefulness of the DBDs. The utilities that have exercised tight control and leadership in their DDR programs have higher quality and more useful documents. In the long term, it would be beneficial for utilities to minimize their reliance on outside engineering organizations to provide the understanding of a facility's engineering design bases and how they were implemented. The team recognized that a utility will always be dependent to some degree on the NSSS vendor and the A/E of record and will certainly need their assistance in developing DBDs. However, it would benefit the utilities if they abandoned the turnkey mentality of being solely plant operators and thoroughly understood the engineering design bases of their facilities. The first step in this transition may be for a utility to assume ownership and control of its DBDs. Heavy reliance on outside organizations to develop DBDs will not bring within the utility a deep understanding or sense of ownership of DBDs.

Once created, the DBDs should be controlled and maintained as-built in a manner similar to other drawings and design documents. Since DBDs by their nature contain engineering design-bases information and configuration-specific descriptive information, it may be necessary to update the DBDs after every modification. Because it is unlikely that the engineering design bases will change frequently, some utilities have tried to decouple the DBDs from the configuration specifics, for example, by including references to facility drawings by drawing number but without the revision number. This is an acceptable concept. Since the drawings are themselves controlled, an engineer requesting a drawing would be typically given the latest revision, unless otherwise specified. It appeared unnecessarily burdensome to have a change in one controlled document result in cascading revisions of other controlled documents. However, when a plant modification results in a change to a DBD, the change should be processed as part of the modification package completion, in the same manner that other affected documents are revised. Because of the important design information contained in the DBDs, it is imperative that all DBD users are informed in a timely manner of DBD changes. Periodic updates on a yearly basis, for example, would not make the DBDs a particularly user-friendly document.

4.2.2 Identification of Missing Design Documentation

Utilities with older plants will generally find design document reconstitution programs more challenging because they typically have not obtained design calculations from their A/E or NSSS vendor and design reconciliation programs were, at best, smaller in scope than those for the newer plants.

Most utilities did not have a systematic method to determine the engineering design bases or system parameters for which calculations should have been performed. Many of the utilities had not identified the parameters or design attributes that were necessary to demonstrate that structures, systems, and components would perform their intended safety functions. Without this up-front identification, it is difficult to determine what documents are missing when the retrieval process is completed. In other words, the utilities were not totally sure which calculations were missing because they did not define the design attributes or controlling design parameters that are necessary to (1) establish and define the functionality and operability requirements of structures, systems, and components, (2) demonstrate the conformance of structures, systems, and components to the design bases, and (3) demonstrate that structures, systems, and components will perform their intended safety function. During the conduct of a DDR program, it is important to determine (1) which design attributes or controlling design parameters lack documentation demonstrating proper implementation, (2) which documents need to be regenerated to demonstrate implementation of the design bases, and (3) the priority in which the documents need to be regenerated. A good approach to accomplish this is to identify a template of design documents before beginning a system or topical design-bases document. A review would then be performed to establish the degree to which the available design documents match the template. Appendix I is an example of typical types of design attributes or controlling design parameters that may be included in a template.

4.2.3 Prioritization of Missing Design Documentation

Once the template has been defined, it is likely that some documentation will be unretrievable. None of the utilities surveyed had a proceduralized, defined prioritization scheme to identify the documents that they felt needed to be regenerated nor a schedule for regeneration to better utilize existing engineering resources. Document regeneration was typically done on a case-by-case basis with reliance placed on the judgment of lead engineers from individual disciplines. In some cases, little thought had been given to the need for document reconstitution. A prioritization methodology should be employed when missing or deficient documents are identified. The methodology should ensure that resources are expeditiously focused on items in a timeframe dictated by their perceived safety significance.

One way the survey team devised to rank the importance of design documents vis-a-vis safety significance is presented in Appendix J. This method divides the design documents into five categories on the basis of their position in the hierarchy of safety systems, with design documents relating to systems covered by the plant technical specifications being considered the most important and placed in Category 1 while documentation to demonstrate the seismic capability of non-safety-related systems from creating a hazard to safety-related systems was placed in Category 5. Utilities that have completed probabalistic risk assessments have used these to quantify the safety significance of safety functions by computing the increase in core-melt probability if, because of missing documentation, it is assumed that a given safety function may not be completed. This also is a reasonable approach to prioritize resources.

4.2.4 Concept of Essential Design Documents

In performing a design document reconstitution program, it is likely that certain design documents will be unretrievable or contain inconsistencies. While the survey team did not see the need to regenerate the complete set of design documents, it is important that certain design documents are available to support plant operation. This set of design documents will be referred to as "essential design documents." It is the opinion of the team that all essential documents be accurate and those that are unretrievable need to be regenerated in an expeditious manner. The team has defined essential design documents as those necessary to support or demonstrate the conservatism of technical specification values, e.g., pump flow calculations and set point calculations and design documents that are necessary both for engineering to support plant operations and for use by the operators to quickly respond to events. Examples of essential documents include, but are not limited to, electrical load lists, set point lists, valve lists, instrument lists, fuse lists, breaker lists, Q-lists, diesel generator load sequencing, P&IDs, flow diagrams, electrical single-line diagrams and schematics and breaker and fuse coordination studies.

4.2.5 Document Regeneration

It would be beneficial to regenerate all missing or inaccurate essential documents in an expeditious manner. If a high level of confidence can be established that the system can fulfill its safety functions through alternate means, such as test data, it may be possible to schedule the regeneration of these documents in a timeframe commensurate with their perceived safety significance. If other supporting information or test data is available to demonstrate that a system, structure, or component can perform its intended safety function, resources expended in the regeneration of missing documentation need to be weighed against other priority safety items, such as those listed on the integrated living schedule for performing plant modifications. For example, it may not be cost-beneficial to regenerate all missing pipe support calculations if, based on reanalysis of a sufficient sample, it can be demonstrated that adequate design margins exist. However, if a modification is proposed that would affect a pipe support then good engineering practice would dictate that it would have to be reanalyzed, if a valid analysis did not exist. The new analysis would then form a point of departure for the proposed modification and quantify the design margin available following the installation of the proposed modification.

4.2.6 Verification of Design-Bases Documents and Validation of Plant Configuration

Many DDR programs did not contain adequate verification or validation of system or topical DBDs. The utility programs were almost uniformly lacking in that DBD source documentation was not technically challenged. The existence of a calculation was presumed sufficient to justify DBD information while the validity of the calculation assumptions, methodology, results, or consistency with the current plant configuration was not vigorously reviewed. Calculations performed before the NRC approval of Appendix B to 10 CFR Part 50 need greater scrutiny. Although calculations performed under approved design verificaton programs may not require as thorough a check, it would be appropriate and prudent to verify that (1) the calculational assumptions are still valid, (2) that any physical data, dimensions, or other design inputs used in a calculation are still valid, and (3) the calculational results appear reasonable on the basis of engineering judgment.

A strong DDR program would include a quality program that assured (1) the retrieved DBD supporting design documents were verified to be valid, (2) any regenerated documents were verified in accordance with existing design verification procedures, (3) the information contained in the system or topical DBDs was verified to have been correctly translated from the supporting design documents, (4) the current plant configuration was validated to be consistent with its DBDs and supporting design documents, and (5) differences between the existing plant configuration and that specified in the DBDs and supporting design documents were reconciled. The most important benefit that could be gained by a utility from a DDR program is the knowledge that the plant is consistent with its design documents and DBDs.

Some utilities have not consistently validated the plant configuration against the system or topical DBDs. This was particularly true for plant-wide design considerations addressed in topical DBDs covering items such as single failure, system interaction, seismic design, and separation requirements, and in validation of component-level design requirements.

It is important that utility verification and validation programs include topical design aspects such as flooding, high-energy line break, seismic, fire protection, and environmental qualification. Although previous utility programs have validated significant portions of these aspects, these earlier programs may not have completely verified all aspects of the system design bases. While some credit can be taken for the earlier efforts, assurance must be gained that previous validation programs were correctly performed and that all necessary aspects of the topical design area have received the requisite validation.

4.3 Operability and Reportability Determinations

The process of determining equipment operability and reportability of design-bases inconsistencies must be a continuous process whereby conclusions regarding operability and reportability are initially made and reevaluated as new or additional information becomes available. This process should begin with the working-level engineers who are involved in the collection, review, and categorization of design-bases information and design documents. It is important that the working-level engineers have sufficient experience to recognize gaps in design documentation that may be indicative of potential operability or reportability concerns and that these be brought quickly to the attention of management for further evaluation in a timeframe commensurate with their safety significance.

4.3.1 Operability Determinations

One of the utility concerns was cycling the plant and [illegible]ing it through perhaps unnecessary power or mode changes because insufficient design documentation was available to conclusively demonstrate that systems or components were operating within their design bases and were therefore considered to be inoperable by the plant technical specifications.

The existence or availability of information to demonstrate that a structure, system, or component is operating within its design bases is not necessarily required to establish operability. Engineering judgment can be relied on to make a preliminary determination of operability and reportability pending further evaluation. The basis for engineering judgments may include operating history; experience with similar structures, systems, and components; preoperational test data; routinely conducted surveillance and testing (to the extent they simulate design-bases conditions); performance of simplified bounding analyses; and other information. In some cases, it may be necessary to regenerate missing design documents to demonstrate conformance with the design bases and to validate engineering judgment.

Implicit in this discussion is the premise of operability; that is, if the system has been operable and meets its surveillance requirements and limiting conditions of operation defined in the plant technical specifications and if there is a reasonable expectation (based on engineering judgment) that the system can perform its intended function, the system should not be immediately considered inoperable solely on the basis of missing documentation. However, the process is not open-ended and the period available to make engineering judgments, perform evaluations persuant to 10 CFR 50.59, or otherwise determine operability, should be bounded by a time commensurate with the safety significance of the open item. It is anticipated that operability judgments will continually need to be reevaluated on the basis of the availability of information. During these periods of evolving information, it may be beneficial to contact the NRC to keep it apprised of the current situation.

4.3.2 Reportability

The 10 CFR 50.2 definition of design bases is used in determining immediate notification requirements under 10 CFR 50.72 and licensee event report requirements under 10 CFR 50.73. These regulations require the licensee to report any event or condition that results in a nuclear power plant being outside its design bases.

Some utilities believe that the number of licensee event reports (LERs) is viewed by certain organizations as an indicator of poor licensee performance without consideration of underlying reasons or the overall benefits in safety and efficiency accrued by performing a DDR program. A related concern was that the potential for reportable items increases as the design bases are more precisely defined by the DBD. This would tend to raise the yearly number of reportable items after the DDR programs are completed. Further, licensees were concerned that the NRC would require reporting of deviations from information contained in DBDs that was part of the commercially driven design constraints but not part of the licensing bases of the facility. The increase in the number of LERs and other reports as required by 10 CFR 50.72 and 50.73 is considered by the licensees as a disincentive for performing a DDR program.

Another concern expressed by licensees related to the timing of reporting missing information that demonstrates conformance to the design bases. For example, during the process of gathering design-bases information it may be initially thought that certain information is unavailable to demonstrate compliance with a particular aspect of the plant's design bases. However, experience with design document reconstitution programs has shown that often information previously thought to be missing is either retrieved or regenerated and it demonstrates that the facility meets its design bases. Licensees wanted to know at what point in the information gathering process is the preparation of a report required pursuant to 10 CFR 50.72 or 10 CFR 50.73.

The reporting requirements specified in 10 CFR 50.9, 50.72, and 50.73 apply equally to discrepancies discovered during DDR programs. Therefore, there is no regulatory basis to treat discrepancies discovered during the conduct of a DDR program differently than any other reportable item. Consequently, reporting suspected but unsubstantiated discrepancies discovered during a DDR program should be handled by the utility in the same manner as other potentially reportable items. While it may be prudent for licensees to informally apprise the NRC of potentially reportable items of high safety significance, formal reporting is not required by the existing regulations until the determination is made by the licensee. As discussed above, the operability and reportability evaluations are closely linked. Therefore, the operability and reportability judgments for each open item could be made in the same timeframe and that timeframe should be commensurate with the perceived safety significance of the item. Generally, once sufficient information becomes available to make the operability determination, the reportability determination should be straightforward.

Utilities also have expressed a desire to combine closely related reportable events in a single LER by supplementing existing LERs. Again, LERs generated during the conduct of a DDR program are no different from other LERs. Guidance has been provided on this question by NUMARC in its "Design Basis Program Guidelines." The subject of supplemental LERs also has been discussed by the NRC in NUREG-1022, "Licensee Event Report System," September 1983, and supplements dated February 1984 and September 1985.

Although it is likely that during the course of performing a DDR program a licensee will generate a larger number of reportable events, from the NRC's standpoint, this will be viewed as a positive indication that a licensee's program is comprehensive. Conversely, the generation of a small number of LERs does not necessarily connote a superficial program. The number of LERs generated during a DDR program will probably be a strong function of the age of the facility and the importance historically placed by the licensee on the availability of design documentation. However, an aggressively implemented design-document reconstitution would be an indication that a particular licensee has recognized the need to have and maintain current certain essential plant design-documents. Although there are regulatory and financial disincentives to conducting an effective DDR program, both perceived and actual, the NRC has in the past encouraged licensee-initiated DDR programs and has, within the framework of existing regulations and regulatory policy, taken certain actions to minimize regulatory disincentives.

The NRC staff recognize that design-bases documents may contain commercially driven design constraints imposed to provide operational flexibility, to facilitate construction, or to realize certain economic benefits. Some of these design constraints do not form the bases for the staff's safety judgment and do not impact the health and safety of the the public. Therefore, deficiencies that are discovered relating to inconsistencies in the application or implementation of such design constraints that are not part of the current licensing bases are not considered reportable under 10 CFR 50.72 or 50.73 simply because the basis of the discrepancy resides in a document the utility calls a DBD. The reportability determination should relate the discrepancy, through a technical evaluation, to the 10 CFR 50.2 definition. In other words, the regulatory design bases are defined in the FSAR and other docketed information not in the system or topical DBDs. To apply an overly conservative reporting interpretation could penalize some utilities that have included useful design information in their DBDs that would not fall within the 10 CFR 50.2 definition of design bases. Conversely, omitting commercially driven design-bases information from DBDs with the thought of limiting reporting obligations will unnecessarily lessen the usefulness of the DBDs.

4.4 Summary

After a plant begins commercial operation, there is a strong economic incentive to shift the emphasis from maintaining engineering excellence to continued operation and maintaining high availability factors. It is important that both are maintained. An internal conflict of interest exists in all utility organizations between the competing interests of maximizing operating revenues and engineering excellence. It is the responsibility of senior utility executives and managers to balance these competing interests. Clearly, events of the recent past have demonstrated that it is shortsighted to sacrifice engineering excellence. Over the long term, striving for and attaining engineering excellence will increase plant availability and plant safety. Overall, the expense of reconstituting the plant's engineering design bases and certain design documents will be justifiable on the basis of economics alone without considering the obvious benefits to plant safety.

5 REFERENCES

American National Standards Institute (ANSI), B-31.1, 1967, "Power Piping," 1430 Broadway, New York, NY 10018.

---, N45.2.9-1974, "Requirements for Collection, Storage, and Maintenance of Quality Assurance Records for Nuclear Power Plants," The American Society of Mechanical Engineers, 345 East 47th Street, New York, NY 10017.

---, N45.2.10-1973, "Quality Assurance Terms and Definitions," The American Society of Mechanical Engineers.

---, N45.2.11-1974, "Quality Assurance Requirements for the Design of Nuclear Power Plants," The American Society of Mechanical Engineers.

---, NQA-1-1989, "Nuclear Quality Assurance Program Requirements for Nuclear Facilities," Supplement S-1, The American Society of Mechanical Engineers.

American Society of Mechanical Engineers (ASME) Boiler and Pressure Vessel Code, Section III, 1977, "Boiler for Construction of Nuclear Power Plant Components," 345 East 47th Street, New York, NY 10017.

---, Section XI, 1986, "Rules for Inservice Inspection of Nuclear Power Plant Components," 345 East 47th Street, New York, NY 10017.

Electrical Power Research Institute, Nuclear Construction Issues Group, NCIG-05, Rev. 1, May 1988, "Guidelines for Piping System Reconciliation," Research Reports Center, Box 50490, Palo Alto, CA 94303.

---, Nuclear Safety Analysis Center, NSAC-39, December 1981, "Verification and Validation of Safety Parameter Display Systems."

---, NSAC-125, May 1989, "Guidelines for 10 CFR 50.59 Safety Evaluations," (also available from Nuclear Management and Resources Council).

Institute of Electrical and Electronics Engineers, IEEE 729-1983, "Software Engineering Technology," 345 East 47th Street, New York, NY 10017.

Nuclear Management and Resources Council, NUMARC 90-12, October 1990, "Design Basis Program Guidelines," 1776 Eye Street, N.W., Washington, DC 20006-2496.

See availability statement on inside front cover for retrievability of NRC documents.

APPENDIX A

SURVEY QUESTIONS

The general survey questions that were provided to the six utilities and the one nuclear supply system (NSSS) vendor are given below. The utility responses were assessed, although not verified, during the surveys. The discipline discussion questions were used during individual meetings with the cognizant discipline personnel to gather information on the utility or NSSS vendor processes.

General Survey Questions

Which organizations prepare, aporove, and issue design documents, such as specifications and drawings, and design change documents, such as design change requests and field change requests?

What are the requirements for incorporating approved design changes into a design document? Is a design document revised and reissued at fixed intervals or revised and reissued when a specified number of approved changes have been issued against the design document?

What design documents are necessary for plant operations and maintained as-built in the control room?

Who determines which design documents are affected by design changes, and who requires revision?

What are the design documents, such as specifications, piping composites, and electrical wiring diagrams, against which design change documents are written?

What methods are used to ensure that design documents are clearly linked to and maintained consistent with safety analyses, licensing commitments, and the design basis?

To what extent is a rigorous ANSI N45.2.11 design verification program employed for modifications?

How are as-found conditions (documented in nonconformance reports, design change requests, and field change requests) that disagree with existing design documents properly identified and reconciled with the documented design basis?

How are minor or temporary modifications properly controlled and given adequate safety evaluations and design verifications?

How is design information coordinated among the utility's operating and engineering staff, the plant architect-engineer, the nuclear steam supplier, and other significant vendors and contractors and consultants?

How do the programs for upkeep of technical procedures, such as operating, maintenance, and testing procedures, incorporate design document requirements?

If a design document reconstitution program is ongoing, what is the level of involvement of the plant architect-engineer and the nuclear steam supplier? How does the the utility control this involvement? If a program is planned, what is the intended level of involvement of the A/E and NSSS supplier, and how will this involvement be controlled?

What discipline-specific types of corporate design procedures, guidelines, standards, and practices are available for the use of design engineers during the development of design changes?

What portion of the engineering of modifications is performed by the utility's in-house technical staff vs. outside contractors?

How are cognizant technical staff made aware of the status and scope of modifications that are planned, or in process, that may interact with other planned or in process modifications? How are these interactions controlled to avoid conflicts between modifications?

How are the necessary and appropriate design documents made available to the preparers of modifications?

What is the utility definition of a design document?

What types of documents (e.g., calculations, drawings, purchase specifications, vendor manuals) does your facility consider to be design documents?

Which design document types does your facility maintain as controlled and which are maintained as-built? How are design documents kept up to date with the as-built plant?

Discipline Discussion Questions

How is design information from modifications integrated into operations and maintenance procedures and training programs? Is this information provided to these organizations in a timely fashion?

What do you believe is the overall effectiveness of the modification program, and what improvements do you believe could be made to enhance the program?

How is the coordination of modifications/design changes between the various involved organizations accomplished?

How is the design/engineering change process initiated?

For those items initiated at the plant level, is the up-front screening process adequate and is it accomplished in a timely fashion?

What is the involvement of operations, maintenance, onsite engineering, and other organizations outside the design organization in the review and implementation of modifications?

What is the backlog of change requests that require engineering action?

Is design documentation (e.g., drawings and calculations) found to be consistent with the plant configuration or are substantial walkdowns and consistency checks required when designing modifications?

What is the experience level of design engineers and reviewers, design managers and safety reviewers? Are "old-timers" available for consultation or input on original design decisions or on underlying reasons for earlier plant modifications? When reconstituting or recreating missing or inadequate design documentation, how do you compensate (or plan to compensate) for inadequacies in the corporate memory?

If changes have been made in the design control and configuration management process over the life of the plant, what reviews have been performed to provide assurance that the documentation, safety analysis, and design decisions for earlier plant modifications are consistent with and adequately support the plant design basis?

APPENDIX B

MATRICES OF DESIGN ATTRIBUTES

The design-attributes matrices are not considered to be a complete list of important design attributes. The matrices were used by the survey team to get a quick overview of the degree of control, retrievability, accessibility, and fidelity of various design attributes and design documents. The attributes include design inputs, design analyses and evaluations, and design outputs. The key to design attributes matrices is given below.

A Not applicable.

B Not retrievable—The documents cannot be located in the utility's files or archives; or the documents can be located, but the information is suspect; or the utility does not recognize the need for such documents.

C Partially retrievable—Some documents can be located, but some of the information is suspect or must be supplemented.

D Completely retrievable—All documents can be located, and are valid.

E Controlled—The documents are within the scope of the utility's document control system.

F Accessible—Documents that are distributed or made accessible to engineering and plant personnel in a controlled manner and are developed to be "user friendly" through format or training.

G As-built—Documents that depict the installed plant configuration.

MECHANICAL COMPONENTS DESIGN ATTRIBUTES MAT[illegible]

DESIGN ATTRIBUTE CATEGORY	A	B	C	D	E	F	G
General Design Criteria							
Safety Classifications							
Regulatory Guides							
Bulletins							
Codes and Standards							
NSSS/BOP Interface Criteria							
System Design Descriptions							
System Functional Criteria and Safety Classifications							
Piping Design Specifications							
Piping Purchase Specifications							
Piping Geometry, Materials and Insulation Data							
Equipment Design Specifications							
Equipment Purchase Specifications							
Equipment Arrangement and Anchorage							
Equipment Geometry and Materials							
Pipe Support Design Specifications							
Pipe Support Purchase Specifications							
Pipe Support Geometry, Materials and Location							
Tornado							
Earthquake							
Flood							
Loss of Coolant Accident (LOCA)							
High Energy Line Break (HELB)							
Moderate Energy Line Break (MELB)							
Environment							
Missiles							
Fluid/Steam Transients							
Vibrat[illegible] Transients							
Seismic Category 2/Category 1							
Fire Protection Pipe							
Buried Pipe							
Differential Building Settlements							
Vendor Equipment Allowable Loads							
Vendor Equipment Functional, Seismic and Environmental Qualification							
Vendor Equipme[illegible] Installation and Maintena[illegible] Requirements							
Vendor Standar[illegible] Component Load Capacities							
Rigorously Analyzed Piping and Supports							
Generically Qualified Piping and Supports							
Typical Support Details and Spacing Criteria for Field Routed Pipe							
Supplementary Steel, Building Steel Load Tracking Program							
Equipment Anchorage Qualification							
Anchor Bolt Load Capacities							
Construction Fabrication, Installation Inspection, and Testing Criteria							
Change Documents							
Modification Packages							

MECHANICAL/NUCLEAR DESIGN ATTRIBUTES MATRIX

DESIGN ATTRIBUTE CATEGORY	A	B	C	D	E	F	G
Design Cycles for Equipment and Systems							
Vibrational Data							
Thermal Expansion Data							
System Flow Requirements							
System Resistance							
Seismic and Environmental Qualification							
Separation Criteria							
Equipment Set Points							
Procedures							
Isometric Drawings							
Calculations							
Analyses							
Specifications							
Vendor Manuals							
Procurement Documentation							
Safety Classification							
Pressure Ratings							
Failure Modes							
Operator Action Requirements							
Normal Operating Parameters							
Environmental Requirements							
Support System Requirements							
Post-Accident Accessibility							
Equipment Ratings							
Materials Selection							
Welding, Fitup Specifications							
Layout and Arrangement							
Isolation Requirements							
Pump Suction and Discharge Pressures							
Surveillance Tests							
Support Loads							
Valve Data							
Valve Stroke Times							
Pump NPSH							
Seismic Categories 2/1 Considerations							
Testing to Post-accident Conditions							

INSTRUMENTATION & CONTROL DESIGN ATTRIBUTES MATRIX

DESIGN ATTRIBUTE CATEGORY	A	B	C	D	E	F	G
Regulatory Requirements (GDCs, Regulatory Guides, NUREGs)							
Bulletins, Notices, Circulars							
FSAR							
Licensing Commitments							
Codes and Standards (IEEE, ISA, ANSI, ASTM, etc.)							
Utility Standards and Practices							
Process System Specifications							
NSSS Interface Criteria							
Vendor Requirements and Manuals							
Calculation Assumptions and Results							
Accident/Transient Analyses							
HELB/MELB Analyses							
ATWS Analysis							
Hazard Analyses							
Tornado							
Missile							
Toxic Gas							
Internal and External Flood							
Freeze							
Fire							
Equipment Qualification							
Thermal/Hydraulic							
Radiation							
Seismic (Categories I and 2/1)							
Vibration							
Functional Requirements							
Channel Purpose/Function							
Interfacing Systems and Functions							
Safety/Quality Class							
Selection of Measured/Controlled Variables							
Control Mode/Strategy							
Range Requirements							
Interlocks/Protection Requirements							
Operator Interface Requirements							
Controls							
Displays							
Alarms							
Trends/Records/Archives							
Bypass Indication							
Post-Event Accessibility							
Survivability Requirements							
Normal Service Environment							
Seismic							
LOCA/HELB							
MELB							
Loss of HVAC							
Tornado							
Missile							

INSTRUMENTATION & CONTROL Continued

DESIGN ATTRIBUTE CATEGORY	A	B	C	D	E	F	G
Flood							
External							
Internal							
Freeze							
Fire/Safe Shutdown							
Vibration							
Local High Temperature							
Normal Radiation							
Surge Withstand/ESD							
Electromagnetic Compatibility							
Performance Requirements							
Preferred Failure Modes							
Reliability/Availability Goals							
Accuracy/Repeatability							
Transient Response							
Testability							
Separation/Independence/Diversity Requirements							
Software Requirements Specifications							
Design-Bases Document							
System							
Topical							
Failure Modes and Effects							
Reliability Analysis							
Trade-Off Evaluations							
Architecture/Configuration							
Instrument Type Selection							
Analog vs. Digital							
Safe Shutdown/Appendix R Analysis							
Shutdown Logic							
Fire Effects Evaluation							
EQ Analysis							
Component Evaluation							
Aging Evaluation							
Qualification Reports/Packages							
Thermal Form Factor							
Internal Heat Rise							
Field Test Reports							
Qualification Reports							
Electromagnetic Compatibility							
Analysis							
Grounding/Shielding Configuration							
Vendor Test Reports							
Field Test Reports							
Surge Withstand Capability							
Vendor Test Reports							
Field Test Reports							
Control Room Design Review							

INSTRUMENTATION & CONTROL Continued

DESIGN ATTRIBUTE CATEGORY	A	B	C	D	E	F	G
Task Analysis							
Alarm Evaluation							
Primary Element Sizing Calculations							
Orifice Cavitation Calculations							
Calibration/Scaling Calculations							
Set Point Tolerance							
Process Set Point Calculations							
Instrument Data							
Channel Tolerance Calculations							
Transient Response Analysis							
Spatial Effects Analysis							
Software Test Reports							
Software Design Analyses							
Verification and Validation Reports							
Piping & Instrumentation Diagrams							
I&C System Specifications							
Instrument Block Diagrams							
Control Logic Diagrams							
Instrument Loop Diagrams (H/W)							
Schematic Connection Diagrams							
Level Setting Diagrams							
Instrument Installation Details							
Rack Internal Arrangement Drawings							
Panel Arrangement Drawings							
Rack Outline/Structural Drawings							
Panel Outline/Structural Drawings							
Tubing Routing Drawings							
Tubing Isometric Drawings							
Equipment Specifications							
Instruments/Devices							
Panels							
Racks							
Connectors							
Equipment Data Sheets							
Installation Specifications							
Setpoint Document							
Instrument Index							
Software Design Specifications							
Source Code							
Software User/Maintenance Documents							

ELECTRICAL DESIGN ATTRIBUTES MATRIX

DESIGN ATTRIBUTE CATEGORY	A	B	C	D	E	F	G
Regulatory Requirements (GDCs, Regulatory Guides, NUREGs)							
Bulletins, Notices, Circulars							
FSAR							
Licensing Commitments							
Codes and Standards (IEEE, NEMA, ANSI, etc.)							
Utility Standards and Practices							
Process System Specifications							
NSSS Interface Criteria							
Vendor Requirements and Manuals							
Calculation Assumptions and Results							
Accident/Transient Analyses							
HELB/MELB Analyses							
Anticipated Transient Without Scram (ATWS) Analysis							
Hazard Analyses							
Tornado							
Missile							
Toxic Gas							
Internal and External Flood							
Freeze							
Fire							
Equipment Qualification							
Thermal/Hydraulic							
Radiation							
Seismic (Categories I and 2/1)							
Vibration							
Functional Requirements							
Interfacing Systems/Functions							
Safety/Quality Class							
Load Purpose/Function							
Load Sequence							
Interlocks/Protection Requirements							
Operator Interface Requirements							
Controls/Displays							
Alarms							
Trends/Records/Archives							
Bypass Indication							
Post-Event Accessibility							
Survivability Requirements							
Normal Service Environment							
Seismic							
LOCA/HELB							
MELB							
Loss of HVAC							
Tornado							
Missile							
Flood							
External							

ELECTRICAL Continued

DESIGN ATTRIBUTE CATEGORY	A	B	C	D	E	F	G
Internal							
Freeze							
Fire/Safe Shutdown							
Vibration							
Local High Temperature							
Normal Radiation							
Surge Withstand Capability							
Lightning							
Performance Requirements							
Preferred Failure Modes							
Reliability/Availability Goals							
System/Component Impedance							
Load Duty Cycle							
Load Electrical Characteristics							
Transient Response							
Testability							
Separation/Independence/Diversity Requirements							
Design-Basis Document							
System							
Topical							
Failure Modes And Effects							
Reliability Analysis							
Trade-Off Evaluations							
Configuration							
Safe Shutdown/Appendix R Analysis							
Shutdown Logic							
Fire Effects Evaluation							
EQ Analysis							
Component Evaluation							
Aging Evaluation							
Qualification Reports/Packages							
Thermal Form Factor							
Internal Heat Rise							
Field Test Reports							
Qualification Reports							
Surge Withstand Capability							
Vendor Test Reports							
Field Test Reports							
Set Point Tolerance							
Electric[illegible] Point Calculations							
Instru[illegible]ta							
Circuit [illegible]nce Calculations							
Separation/Isolation Analyses							
Lightning Protection Analyses							
Emergency Lighting Calculations							
Load Flow Calculations							
Short Circuit Calculations							

ELECTRICAL Continued

DESIGN ATTRIBUTE CATEGORY	A	B	C	D	E	F	G
Motor Starting Calculations							
Medium Voltage ac							
Low Voltage ac							
120 Vac							
125 Vdc							
System Transient Analysis							
Protective Device Coordination							
Medium Voltage ac							
Low Voltage ac							
120 Vac							
125 Vdc							
Degraded Voltage Analysis							
Station Blackout Analysis							
Offsite/Onsite Independence							
Load Sequence/Timing Calculations							
Diesel Generator Sizing Calculations							
Battery Sizing Calculations							
Battery H_2 Generation							
Battery Recharging Time							
Charger Sizing Calculations							
Inverter Sizing Calculations							
Transformer Sizing Calculations							
Fuse Rating Calculations							
Grounding Impedance Calculations							
Load Rating Calculations							
Motor Acceleration Calculations							
Motor Overload Sizing							
Cable Ampacity Calculations							
Cable Pulling Calculations							
Raceway Loading Calculations							
Electrical Penetration Calculations							
Panelboard Derating Calculations							
Heat Tracing Calculations							
MOV Actuator Sizing Calculations							
Electrical System Specifications							
Medium Voltage ac							
Low Voltage ac							
120 Vac							
125 Vdc							
One-Line Diagrams							
Medium Voltage ac							
Low Voltage ac							
120 Vac							
125 Vdc							
Control Logic Diagrams							
Schematic Connection Diagrams							
Internal Wiring Diagrams							
Three-Line Diagrams							

ELECTRICAL Continued

DESIGN ATTRIBUTE CATEGORY	A	B	C	D	E	F	G
Electrical Arrangement Drawings							
Raceway Layout Drawings							
Enclosure Internal Arrangements							
Panel Arrangement Drawings							
Enclosure Outline/Structural Drawings							
Panel Outline/Structural Drawings							
Cable and Raceway Schedule							
Conduit/Tray Plans							
Conduit/Tray Details							
Grounding Plans/Details							
Electrical Installation Details							
Equipment Specifications							
Equipment Data Sheets							
Wire/Cable Specifications							
Power Supply Specifications							
Installation Specifications							
Motor and Load Data/List							
Medium Voltage ac							
Low Voltage ac							
120 Vac							
125 Vdc							
Transformer Tap Settings							
Protective Device Settings							
Medium Voltage ac							
Low Voltage ac							
120 Vac							
125 Vdc							
Fuse Characteristics and Ratings							
Heat Dissipation Data							
Q-List							

APPENDIX C

DRAWING PRIORITIZATION METHODOLOGY

Most utilities surveyed use a prioritization methodology to schedule drawing revisions. Typical categories for prioritizing drawings are given below.

Priority 1: This category contains drawings defined by the operations organization as critical to plant operations. These drawings are updated as part of the turnover process and available in the control room. This set of drawings consists of piping and instrumentation diagrams (P&IDs), one-line electrical diagrams, logic diagrams, valve index and circuit breaker list diagrams.

Priority 2: This category contains control room drawings defined by the operations organization as second-tier operating documents. These drawings are updated and available in the control room within 30 days from the time a system has become operational. This set of drawings consists of elementary wiring diagrams and schematics, P&IDs (not included in Priority 1), and instrument loop diagrams.

Priority 3: This category contains drawings and documents defined by the maintenance organization (not included in Priority 1 and 2 above) as critical to plant maintenance. These drawings are updated within 60 days from the time operations has accepted a system. However, these drawings are not available in the control room. This set of drawings consists of electrical connection diagrams, internal wiring diagrams, cable and raceway schedule, lighting and raceway drawings, selected vendor drawings that contain maintenance information, Q-list and EQ-list (equipment qualification list of components), total equipment data base, and pipe hanger drawings.

Priority 4: This category contains drawings and documents defined by the engineering organization (not included in Priority 1 through 3) as critical to engineering. These drawings are updated within 90 days from the time operations accepts a system. This set of drawings consists of documents related to Appendix R criteria, piping isometrics, welding procedures, security hardware, equipment list, heat-balance diagram, yard piping, and specifications.

Priority 5: This category contains the remaining drawings and documents that are not identified in Priorities 1 through 4. These documents are updated on an as-requested basis within 180 days after the request is received. This set of drawings consists of historical information on erection drawings, drawings such as piping plan views and those drawings unlikely to be affected by a design change such as component outlines, printed circuit card schematics, foundations, and masonry.

APPENDIX D

AVAILABILITY OF
INTERNAL DESIGN GUIDANCE DOCUMENTS

The six utilities surveyed summarized the availability of their design guidance documents that were either maintained in-house or planned to be available in-house. Documents maintained by contracted organizations were not included.

Topics covered by utility design guides, standards, or specifications are given below.

Mechanical/Nuclear

Hydraulic calculation methodology
Physical separation
Single-failure analysis
Materials selection
Component design specifications
Component procurement specifications
Welding and fitup specifications
Installation details and specifications

Electrical

System calculation methodology
Conductor sizing
Overload sizing
Protective device application
Electrical separation/isolation
Failure analysis
Reliability analysis
Appendix R compliance
Raceway design
Lightning protection
General procurement specifications
Installation details and specifications

Instrumentation

Control strategy
Instrument selection/application
Primary element sizing
Operator interface
Separation/isolation
Failure analysis
Reliability analysis
Equipment qualification
Electromagnetic compatibility
Surge withstand capability
Set point tolerance
Software design verification and validation
General procurement specifications
Installation details and specifications

Mechanical Components

Piping design specifications
Piping procurement specifications
Equipment design specifications
Equipment procurement specifications
Equipment arrangement/anchorage
Pipe support design specifications
Pipe support procurement specifications
Support details/installation

APPENDIX E

METHODOLOGY FOR DETERMINING IMPORTANT SYSTEM, STRUCTURE, AND COMPONENT FUNCTIONS, PARAMETERS, AND INTERFACES

Florida Power Corporation has given the NRC permission to include an example of its template approach to identifying the design attributes or controlling design parameters of important structures, systems, and components to perform their intended safety functions. System logic trees and design-bases functional diagrams are used in this identification process.

The utility stated that*

- System logic trees serve as an outline for the development of the design-bases document (DBD) for their particular system. For each safety function of the system, a tree is generated that diagrammatically depicts the regulatory requirements for the function and the supporting system/component requirements. The regulatory requirements (e.g., general design criteria and standards) are the current licensing bases for the function identified. The system requirements (system parameters) are the activities the system must perform to support the function and the component requirements (component parameters) are the necessary components and actions required to support the system requirements. The DBD developer can then use the logic trees for a particular system to identify the required system/component parameters (i.e., numerical values) associated with the listed requirements. The trees also help to identify the source documents that will be needed for the DBD.

- Shutdown logic diagrams (SLDs) graphically depict the plant responses at the system level to those events postulated in a plant's final safety analysis report. Each SLD identifies those systems essential to safe shutdown following an event, as credited in the plant's safety analysis. Each system appearing on an SLD supports one or more of the safety functions necessary to achieve and maintain safe shutdown following the postulated event. System interfaces and the safety function supported by each system also are identified on each SLD.

  For each system identified on an SLD, a safety function diagram (SFD) is then created. The SFDs present in logic diagram format the complete set of equipment that must function in order for the applicable system to fulfill its design-basis safety functions in support of safe shutdown. The presentation of these diagrams comes in two parts, the composite and the details.

  On the SFD composite, all of the active components and significant passive components required for the system to operate in response to an analyzed event, as shown on the SLDs, are represented by appropriate symbols. Thus, the composite graphically portrays the minimum set of equipment needed for the system to satisfy its safety design

---

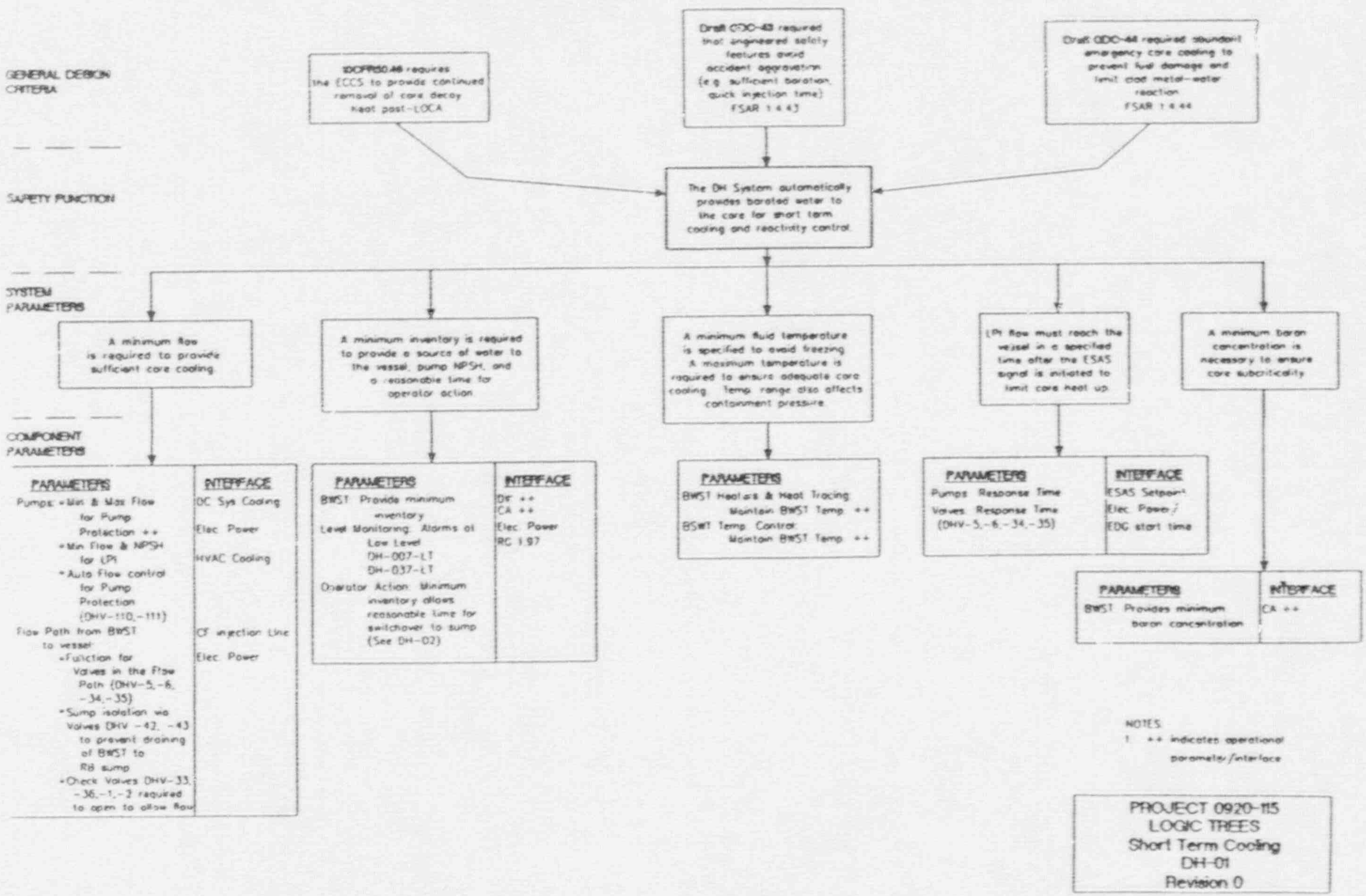
* Source: Florida Power Corporation letter (NEA 90-1224) of August 6, 1990, from K. B. Baker to Eugene V. Imbro, NRC

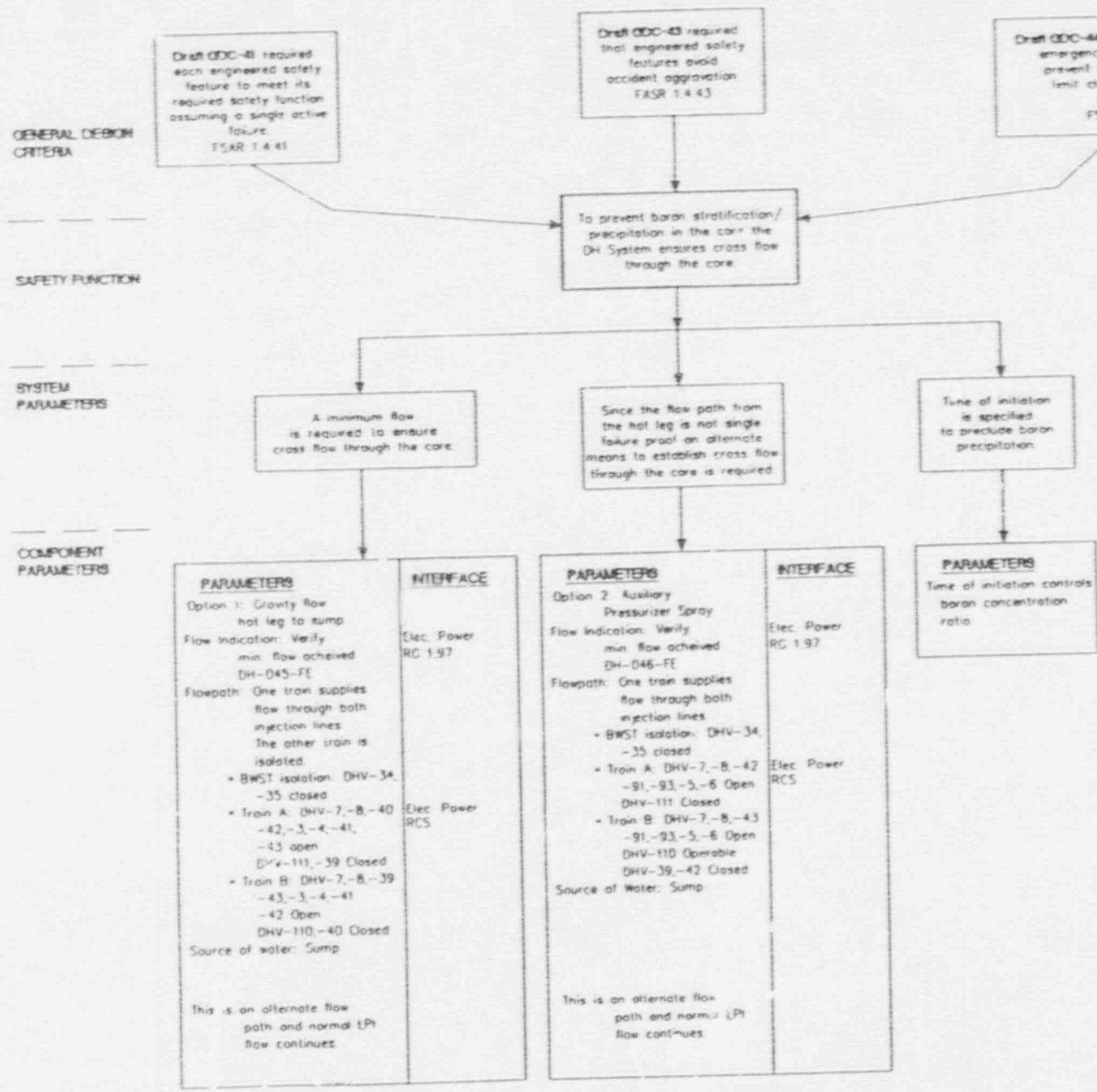
requirements. In addition, support requirements from interfacing systems, such as cooling or lubrication systems, are shown within the system composite.

For those system components that require supporting equipment for operation (i.e., complex components), an SFD detail is developed to display the role of the supporting/interfacing equipment. The detail drawings display in logic diagram format the plant equipment needed to support operation of each of the essential system components identified on the system composite SFD. As such, the detail drawings also show the interfaces that exist between systems and that are required for system operability. For instance, instrumentation and control inputs, isolation signals, and actuation signals that are provided by other systems are identified on the details. This, the SFD details include transmitters, limit switches, and other interfacing devices necessary for control of equipment identified on the composites.

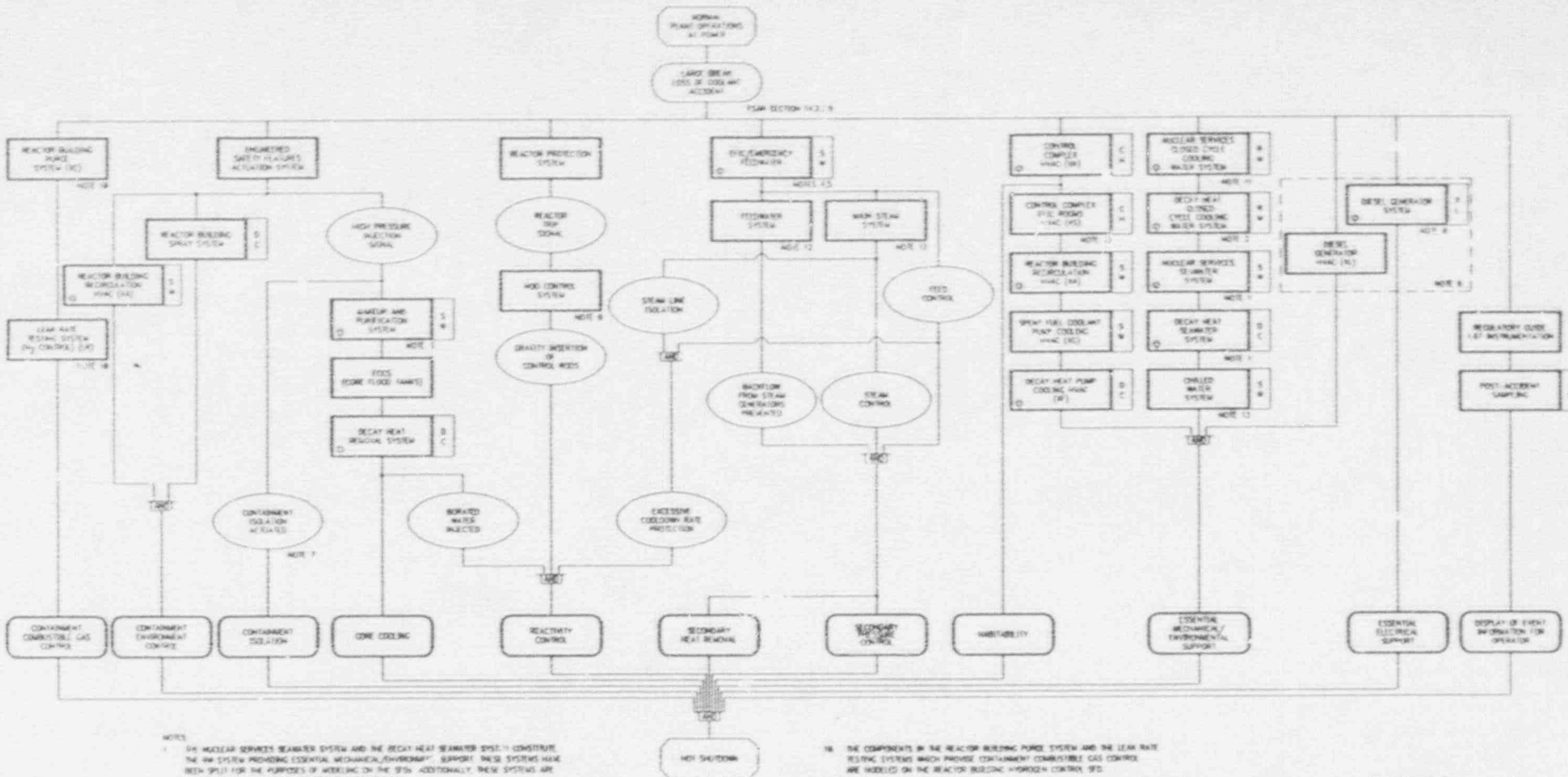
The SLDs and SFDs combined depict all systems and components necessary for mitigation of the consequences of FSAR postulated accidents.

Examples of the logic trees and diagrams follow.


GENERAL DESIGN CRITERIA
SAFETY FUNCTION
SYSTEM PARAMETERS
COMPONENT PARAMETERS
10CFR50.46 requires the ECCS to provide continued removal of core decay heat post-LOCA
Draft GDC-43 required that engineered safety features avoid accident aggravation (e.g. sufficient boration, quick injection time) FSAR 1.4.43
Draft GDC-44 required abundant emergency core cooling to prevent fuel damage and limit clad metal-water reaction. FSAR 1.4.44
The DH System automatically provides borated water to the core for short term cooling and reactivity control.
A minimum flow is required to provide sufficient core cooling.
A minimum inventory is required to provide a source of water to the vessel, pump NPSH, and a reasonable time for operator action.
A minimum fluid temperature is specified to avoid freezing. A maximum temperature is required to ensure adequate core cooling. Temp. range also affects containment pressure.
LPI flow must reach the vessel in a specified time after the ESAS signal is initiated to limit core heat up.
A minimum boron concentration is necessary to ensure core subcriticality.
PARAMETERS
Pumps: •Min & Max Flow for Pump Protection ++
•Min Flow & NPSH for LPI
•Auto Flow control for Pump Protection (DHV-110,-111)
Flow Path from BWST to vessel
•Function for Valves in the Flow Path (DHV-5,-6,-34,-35)
•Sump isolation via Valves DHV-42, -43 to prevent draining of BWST to RB sump
•Check Valves DHV-33, -36,-1,-2 required to open to allow flow
INTERFACE
DC Sys Cooling
Elec. Power
HVAC Cooling
CF injection Line
Elec. Power
PARAMETERS
BWST: Provide minimum inventory
Level Monitoring: Alarms at Low Level DH-007-LT DH-037-LT
Operator Action: Minimum inventory allows reasonable time for switchover to sump (See DH-02)
INTERFACE
DH ++
CA ++
Elec. Power
RG 1.97
PARAMETERS
BWST Heaters & Heat Tracing: Maintain BWST Temp. ++
BSWT Temp. Control: Maintain BWST Temp. ++
PARAMETERS
Pumps: Response Time
Valves: Response Time (DHV-5,-6,-34,-35)
INTERFACE
ESAS Setpoint
Elec. Power
EDG start time
PARAMETERS
BWST: Provides minimum boron concentration
INTERFACE
CA ++
NOTES:
1. ++ indicates operational parameter/interface
PROJECT 0920-115
LOGIC TREES
Short Term Cooling
DH-01
Revision 0



PROJECT 0920-115
LOGIC TREES
Boron Precipitation Prevention
DH-04
Revision 0



NOTES:

1. THE NUCLEAR SERVICES SEAWATER SYSTEM AND THE DECAY HEAT SEAWATER SYSTEM CONSTITUTE THE SW SYSTEM PROVIDING ESSENTIAL MECHANICAL/ENVIRONMENTAL SUPPORT. THESE SYSTEMS HAVE BEEN SPLIT FOR THE PURPOSES OF MODELING ON THE SFDs. ADDITIONALLY, THESE SYSTEMS ARE DEPENDENT ON EACH OTHER FOR PROPER PUMP COOLING.
2. THE DECAY HEAT CLOSED CYCLE COOLING WATER SYSTEM IS ALSO SUPPORTED BY THE DECAY HEAT PUMP COOLING HVAC SYSTEM.
3. MUP-1B CAN ONLY BE COOLED BY THE SW SYSTEM. HOWEVER, MUP-1A AND MUP-1C CAN BE COOLED BY EITHER SW OR DC SYSTEMS.
4. THE EMERGENCY FEEDWATER SYSTEM IS INCLUDED FOR SECONDARY HEAT REMOVAL AND PRESSURE CONTROL. HOWEVER, FOLLOWING EXTREMELY LARGE RCS BREAKS, ITS EFFECT WOULD BE NEGLIGIBLE AND WAS THEREFORE NOT CONSIDERED IN THE SAFETY ANALYSIS. SIMILARLY, FOLLOWING LARGE BREAKS, THE EFFECTIVE DECOUPLING OF THE SECONDARY FROM THE PRIMARY SYSTEM MINIMIZES THE STEAM AND FEED FLOW RATE EFFECTS ON RCS COOLDOWN AND CORE REACTIVITY.
5. THE MAIN AND AUXILIARY STEAM SYSTEMS ALSO SUPPORT THE OPERATION OF THE TURBINE DRIVEN EMERGENCY FEEDWATER PUMP.
6. THIS PORTION OF THE LOGIC IS APPLICABLE WHEN THERE IS A COINCIDENT LOSS OF OFFSITE POWER.
7. THE CONTAINMENT ISOLATION VALVES, WHICH ACTUATE ON HIGH REACTOR BUILDING PRESSURE, ALONG WITH THOSE WHICH CLOSE FOR HPI DIVERSE CONTAINMENT ISOLATION WILL ACCOMPLISH THE REQUIRED CONTAINMENT ISOLATION.
8. THE DIESEL FUEL (DF), THE DIESEL GENERATOR COOLANT (DJ), AND THE DIESEL GENERATOR LUBE OIL (DL) SYSTEMS ARE MODELED WITHIN THE DIESEL GENERATOR SFD.
9. PER B&W TOPICAL REPORT BAW-10103A, REVISION 3, WHEN ANALYZING POWER GENERATED WITHIN THE CORE DURING A LOCA, NO CREDIT IS TAKEN FOR THE REACTOR TRIP FOR BREAKS WITH A LEAK AREA GREATER THAN 0.5 FT².
10. THE COMPONENTS IN THE REACTOR BUILDING PURGE SYSTEM AND THE LEAK RATE TESTING SYSTEMS WHICH PROVIDE CONTAINMENT COMBUSTIBLE GAS CONTROL ARE MODELED ON THE REACTOR BUILDING HYDROGEN CONTROL SFD.
11. THE NUCLEAR SERVICES CLOSED CYCLE COOLING WATER SYSTEM IS ALSO SUPPORTED BY THE CHILLED WATER SYSTEM.
12. FOLLOWING A REACTOR TRIP, MANUAL ISOLATION OF THE MAIN FEEDWATER LINES AND THE MAIN STEAM LINES PROVIDES A MEANS TO CONTROL THE RATE OF SECONDARY HEAT REMOVAL.
13. THE EFIC ROOMS HVAC AND THE CHILLED WATER SYSTEM ARE MODELED WITHIN THE CONTROL COMPLEX HVAC SFD.

PRELIMINARY
FOR INFORMATION ONLY
THIS DIAGRAM REFLECTS PLANT CONFIGURATION AS OF AUGUST 9, 1988

REVISIONS	BY	CHECKED	APPROVED	DATE

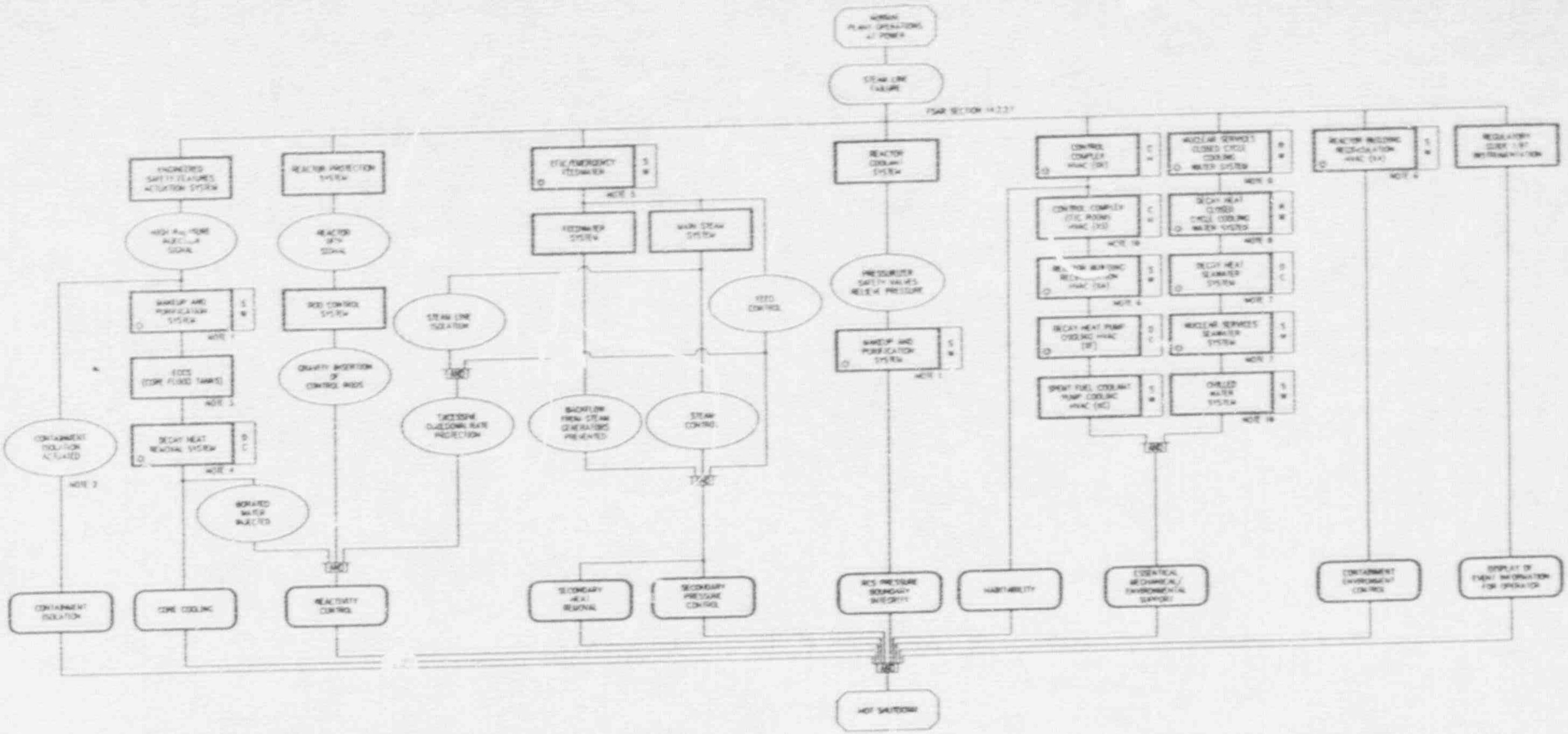
FLORIDA POWER CORPORATION
ST. PETERSBURG, FLORIDA
CRYSTAL RIVER PLANT
UNIT NO.3 855,000 KW

SHUTDOWN LOGIC DIAGRAM
LARGE BREAK LOSS OF COOLANT ACCIDENT

IMPELL

DRAWN BY ______ DATE ______
CHECKED BY ______ DATE ______
APPROVED BY ______ DATE ______

0920-136-SLD1 — SHEET 1 OF 1 — DRAWING NUMBER — REV. B — SCALE



NOTES:

1. MUP-1B CAN ONLY BE COOLED BY THE SW SYSTEM. HOWEVER, MUP-1A AND MUP-1C CAN BE COOLED BY EITHER SW OR DC SYSTEMS.
2. FOR A STEAM LINE BREAK OUTSIDE CONTAINMENT, ONLY THE CONTAINMENT ISOLATION VALVES IN THOSE SYSTEMS NOT REQUIRED FOR RCS OR CONTAINMENT HEAT REMOVAL ARE ISOLATED UPON HPI ACTUATION.
3. FSAR CHAPTER 14 TAKES CREDIT FOR THE BORON CONTENT OF HPI AND CORE FLOOD TANK INJECTION IN ONE ANALYZED MSLB SCENARIO.
4. THE DECAY HEAT PUMPS (LPI) WILL ACTUATE UPON THE HPI SIGNAL BUT WILL RUN IN THE RECIRCULATION MODE UNTIL THE RCS PRESSURE DECREASES TO LESS THAN PUMP SHUTOFF HEAD.
5. THE MAIN AND AUXILIARY STEAM SYSTEMS ALSO SUPPORT THE OPERATION OF THE TURBINE DRIVEN EMERGENCY FEEDWATER PUMP. THE EFW SYSTEM IS ACTUATED VIA EFIC UPON LOW STEAM GENERATOR PRESSURE FOLLOWING THIS EVENT.
6. ALTHOUGH THE REACTOR BUILDING RECIRCULATION SYSTEM IS NORMALLY COOLED BY THE INDUSTRIAL COOLER, NUCLEAR SERVICES CLOSED CYCLE COOLING WATER PROVIDES THE SAFETY GRADE COOLING MECHANISM. HOWEVER, FOLLOWING A STEAMLINE FAILURE OUTSIDE CONTAINMENT REALIGNMENT TO THIS COOLING WATER SUPPLY WOULD NOT BE AUTOMATIC SINCE REACTOR BUILDING PRESSURE WOULD NOT REACH THE HIGH PRESSURE ACTUATION SETPOINT.
7. THE NUCLEAR SERVICES SEAWATER SYSTEM AND THE DECAY HEAT SEAWATER SYSTEM CONSTITUTE THE RW SYSTEM PROVIDING ESSENTIAL MECHANICAL/ENVIRONMENT SUPPORT. THESE SYSTEMS HAVE BEEN SPLIT FOR THE PURPOSES OF MODELING ON THE SLDs. ADDITIONALLY, THESE SYSTEMS ARE DEPENDENT ON EACH OTHER FOR PROPER PUMP COOLING.
8. THE DECAY HEAT CLOSED CYCLE COOLING WATER SYSTEM IS ALSO SUPPORTED BY THE DECAY HEAT PUMP COOLING HVAC SYSTEM.
9. THE NUCLEAR SERVICES CLOSED CYCLE COOLING WATER SYSTEM IS ALSO SUPPORTED BY THE CHILLED WATER SYSTEM.
10. THE EFIC ROOMS HVAC AND THE CHILLED WATER SYSTEM ARE MODELED WITHIN THE CONTROL COMPLEX HVAC SLD.

PRELIMINARY
FOR INFORMATION ONLY
THIS DIAGRAM REFLECTS PLANT CONFIGURATION AS OF AUGUST 8, 1988

NO.	REVISIONS	BY	CHECKED	APPROVED	DATE

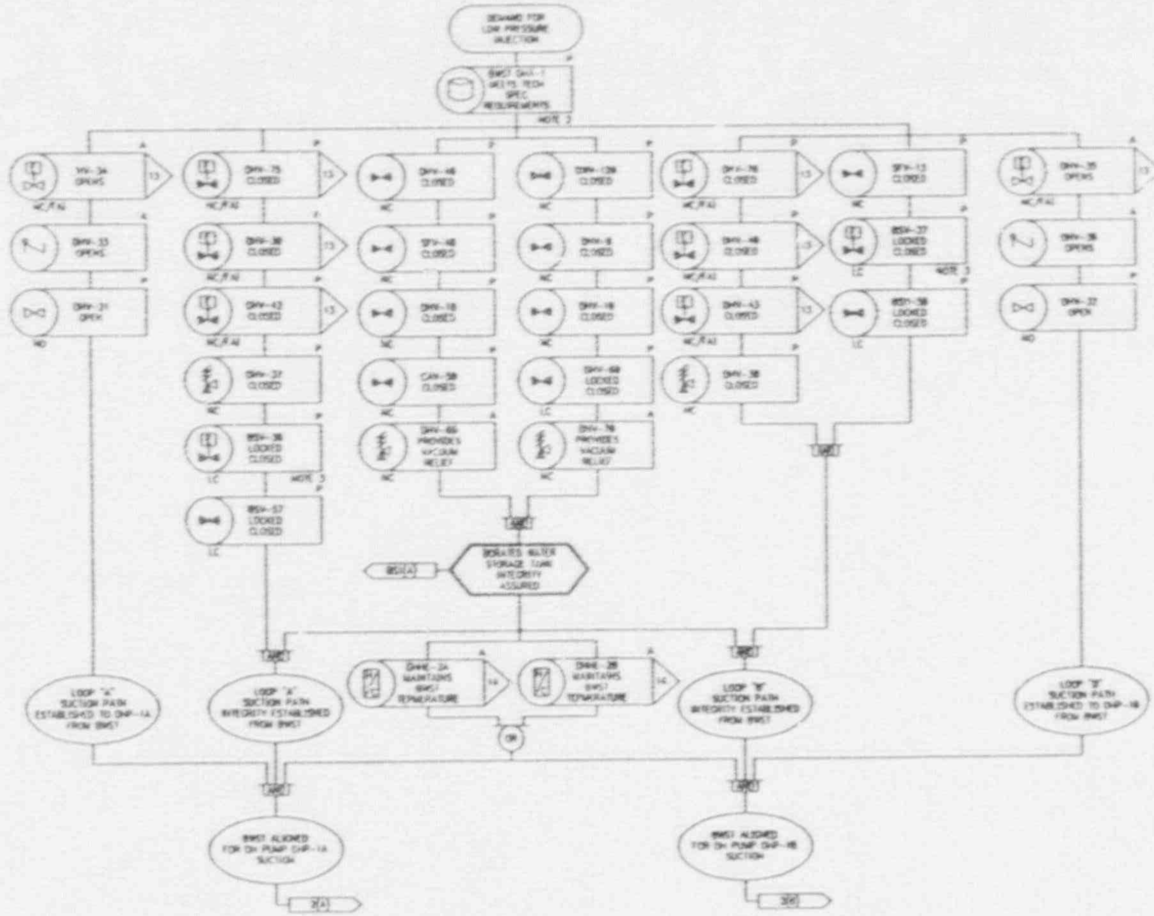
FLORIDA POWER CORPORATION
ST. PETERSBURG, FLORIDA
CRYSTAL RIVER PLANT
UNIT NO. 3 — 855,000 KW

SHUTDOWN LOGIC DIAGRAM
STEAM LINE
FAILURE

IMPELL

DRAWN BY ______ DATE ______
CHECKED BY ______ DATE ______
APPROVED BY ______ DATE ______

SCALE | 0920-136-SLD4 | SHEET 1 OF 1 | DRAWING NUMBER | REV. 0



NOTES:

1. THIS COMPOSITE DEPICTS THE DH SYSTEM COMPONENT FUNCTIONS TO PROVIDE BORATED WATER TO THE CORE FOR SHORTTERM COOLING AND REACTIVITY CONTROL. NO OPERATOR ACTION IS NECESSARY IN THIS MODE.
2. TECHNICAL SPECIFICATIONS GOVERN TANK LEVEL, TEMPERATURE, AND BORON CONCENTRATION.
3. THE BREAKER FOR THIS VALVE IS NORMALLY IN LOCK RESET, PREVENTING INADVERTANT OPENING OF THE VALVE. THEREFORE, NO DETAIL IS PROVIDED FOR THIS VALVE. THE VALVE IS ALSO LOCKED CLOSED BY HANDWHEEL.

PRELIMINARY
FOR INFORMATION ONLY
THIS DIAGRAM REFLECTS PLANT CONFIGURATION AS OF AUGUST 4, 1989

NO.	REVISIONS	BY	CHECKED	APPROVED	DATE

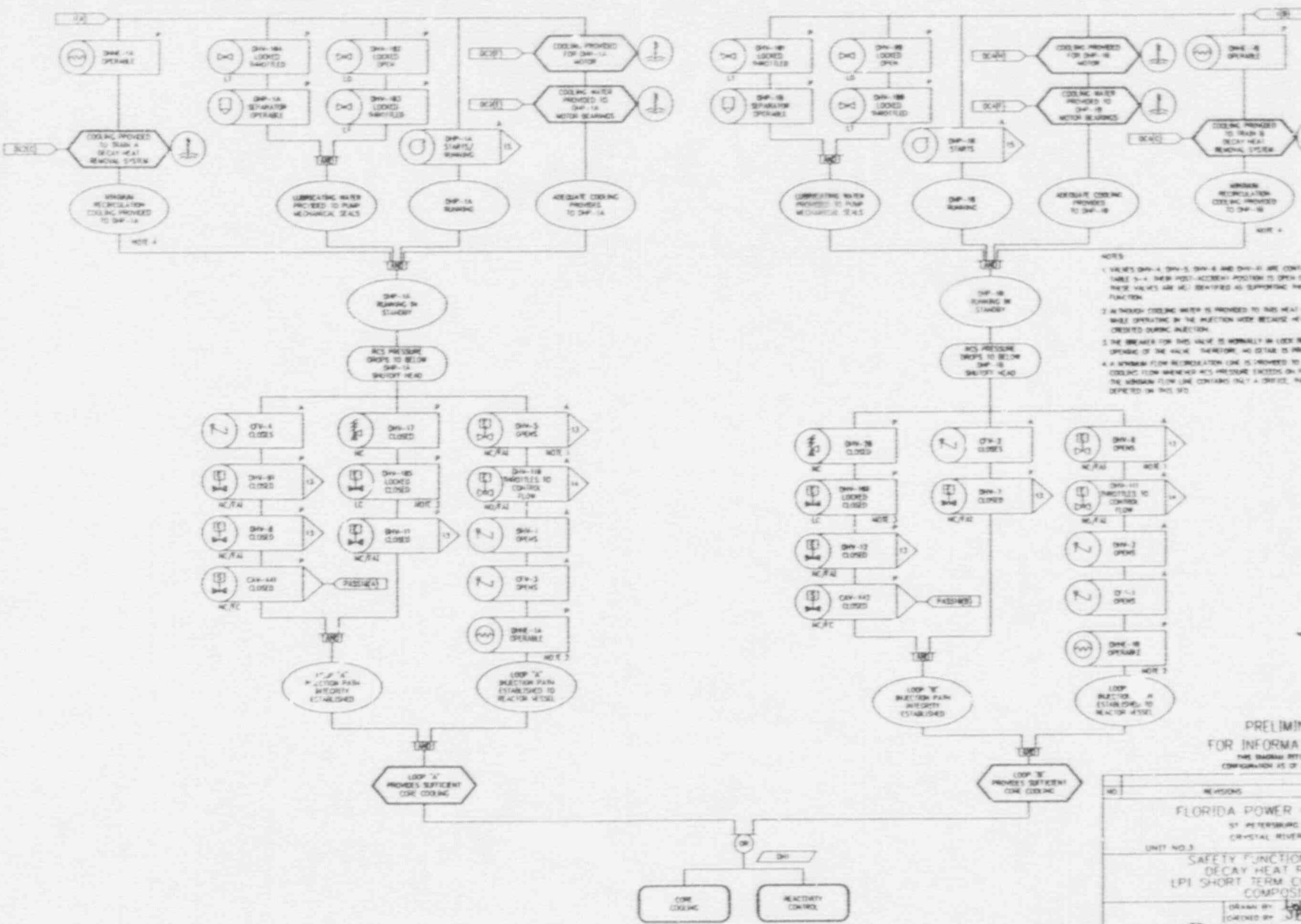
FLORIDA POWER CORPORATION
ST. PETERSBURG, FLORIDA
CRYSTAL RIVER PLANT
UNIT NO. 3 — 855,000 KW

SAFETY FUNCTION DIAGRAM
DECAY HEAT REMOVAL
LPI SHORT TERM COOLING MODE
COMPOSITE

IMPELL

DRAWN BY: LWA — DATE: 27MAR90
CHECKED BY: JBH — DATE: 27MAR90
APPROVED BY: — DATE:

0920-136-DH
SHEET 1 OF 15
DRAWING NUMBER — REV B
SCALE



NOTES:

1. VALVES DHV-4, DHV-5, DHV-6 AND DHV-41 ARE CONTAINMENT ISOLATION VALVES PER FSAR TABLE 5-4. THEIR POST-ACCIDENT POSITION IS OPEN DURING SOME MODES OF LPI; THEREFORE, THESE VALVES ARE NOT IDENTIFIED AS SUPPORTING THE CONTAINMENT ISOLATION SAFETY FUNCTION.
2. ALTHOUGH COOLING WATER IS PROVIDED TO THIS HEAT EXCHANGER, IT IS NOT NEEDED WHILE OPERATING IN THE INJECTION MODE BECAUSE HEAT REMOVAL IS NOT CREDITED DURING INJECTION.
3. THE BREAKER FOR THIS VALVE IS NORMALLY IN LOCK RESET, PREVENTING INADVERTANT OPENING OF THE VALVE. THEREFORE, NO ESTAB IS PROVIDED FOR THIS VALVE.
4. A MINIMUM FLOW RECIRCULATION LINE IS PROVIDED TO ALLOW FOR PUMP COOLING FLOW WHENEVER RCS PRESSURE EXCEEDS DH PUMP SHUTOFF HEAD. THE MINIMUM FLOW LINE CONTAINS ONLY A ORIFICE, THEREFORE, IS NOT DEPICTED ON THIS SFD.

PRELIMINARY
FOR INFORMATION ONLY
THIS DIAGRAM REFLECTS PLANT CONFIGURATION AS OF AUGUST 8, 1989

NO.	REVISIONS	BY	CHECKED	APPROVED	DATE

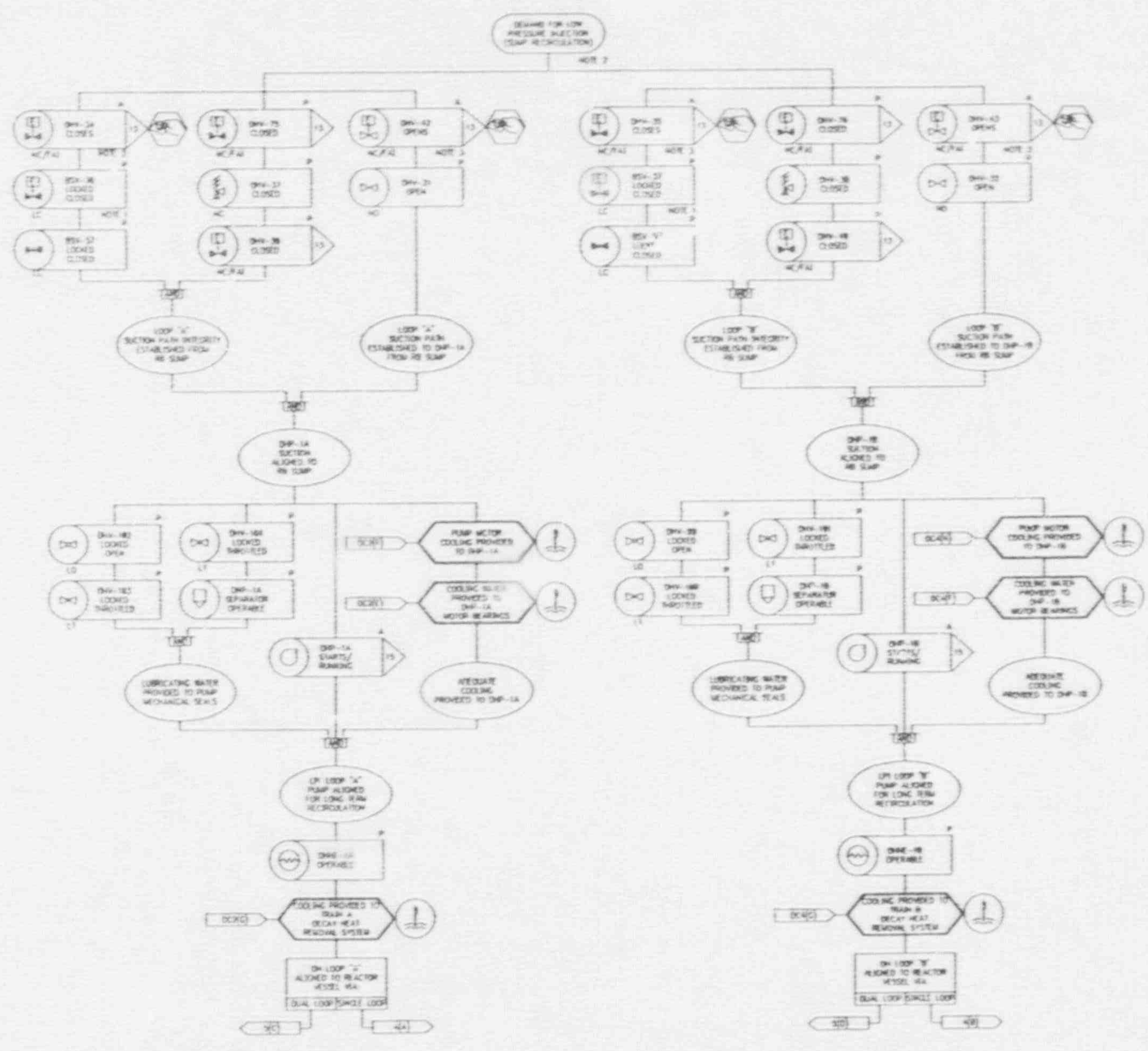
FLORIDA POWER CORPORATION
ST. PETERSBURG, FLORIDA
CRYSTAL RIVER PLANT
UNIT NO. 3 — 855,000 KW

SAFETY FUNCTION DIAGRAM
DECAY HEAT REMOVAL
LPI SHORT TERM COOLING MODE
COMPOSITE

DRAWN BY: LWH — DATE: 27 MAR 90
CHECKED BY: JBH — DATE: 27 MAR 90
APPROVED BY: — DATE:

IMPELL

DRAWING NUMBER: 0920-136-DH, SHEET 2 OF 15 — REV. 0
SCALE



NOTES:

1. THE BREAKER FOR THIS VALVE IS NORMALLY IN LOCK RESET, PREVENTING INADVERTANT OPENING OF THE VALVE. THEREFORE, NO DETAIL IS PROVIDED FOR THIS VALVE. THE VALVE IS ALSO LOCKED CLOSED BY HANDWHEEL.
2. THIS COMPOSITE DEPICTS THE DH SYSTEM COMPONENT FUNCTIONS NECESSARY TO SHIFT FROM LPI INJECTION MODE TO LPI RECIRCULATION MODE. THUS, THE INITIAL CONDITION ASSUMED FOR THIS DRAWING IS DH SYSTEM OPERATING IN LPI INJECTION MODE.
3. ONCE BWST LEVEL REACHES 2.5 FEET, LPI SUCTION SHOULD BE SHIFTED TO THE RB SUMP. THE SEQUENCE OF OPERATION OF DHV-34,35 AND DHV-42,43 MUST BE DONE CAREFULLY TO AVOID LOSING SUCTION TO THE DHPS. DHV-42, -43 WILL BE OPENED FIRST, SUCH THAT ALL FOUR SUCTION ISOLATION VALVES ARE OPEN SIMULTANEOUSLY. THEN DHV-34, -35 WILL BE CLOSED.

PRELIMINARY
FOR INFORMATION ONLY
THIS DIAGRAM REFLECTS PLANT CONFIGURATION AS OF AUGUST 9, 1989

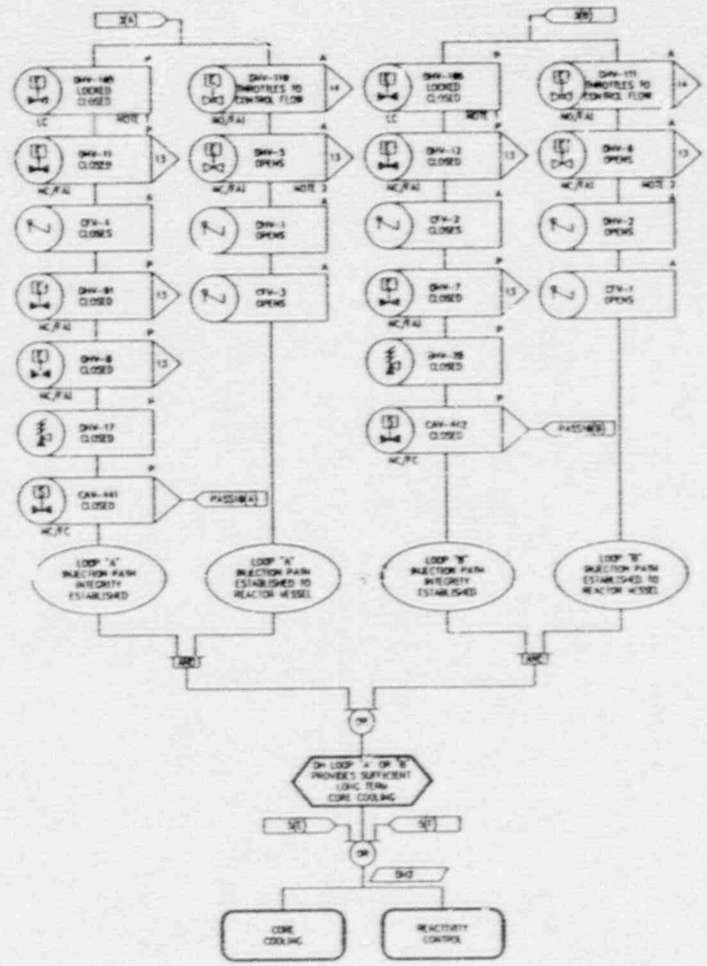
NO.	REVISIONS	BY	CHECKED	APPROVED	DATE

FLORIDA POWER CORPORATION
ST. PETERSBURG, FLORIDA
CRYSTAL RIVER PLANT
UNIT NO. 3 — 855,000 KW

SAFETY FUNCTION DIAGRAM
DECAY HEAT REMOVAL
LPI LONG TERM COOLING MODE
COMPOSITE

IMPELL

DRAWN BY: LWB DATE: 21AUG89
CHECKED BY: GBH DATE: 21AUG89
APPROVED BY: DATE:
SCALE
0920-136-DH
SHEET 3 OF 15
DRAWING NUMBER
REV. 3



NOTES

1. THE BREAKER FOR THIS VALVE IS NORMALLY IN LOCK RESET, PREVENTING INADVERTANT OPENING OF THE VALVE. THEREFORE, NO DETAIL IS PROVIDED FOR THIS VALVE.
2. VALVES DHV-4, DHV-5, DHV-6 AND DHV-41 ARE CONTAINMENT ISOLATION VALVES PER FSAR TABLE 5-4. THEIR POST-ACCIDENT POSITION IS OPEN DURING SOME MODES OF LPI. THEREFORE THESE VALVES ARE NOT IDENTIFIED AS SUPPORTING THE CONTAINMENT ISOLATION SAFETY FUNCTION.

PRELIMINARY
FOR INFORMATION ONLY
THIS DIAGRAM REFLECTS PLANT CONFIGURATION AS OF AUGUST 8, 1988

NO	REVISIONS	BY	CHECKED	APPROVED	DATE

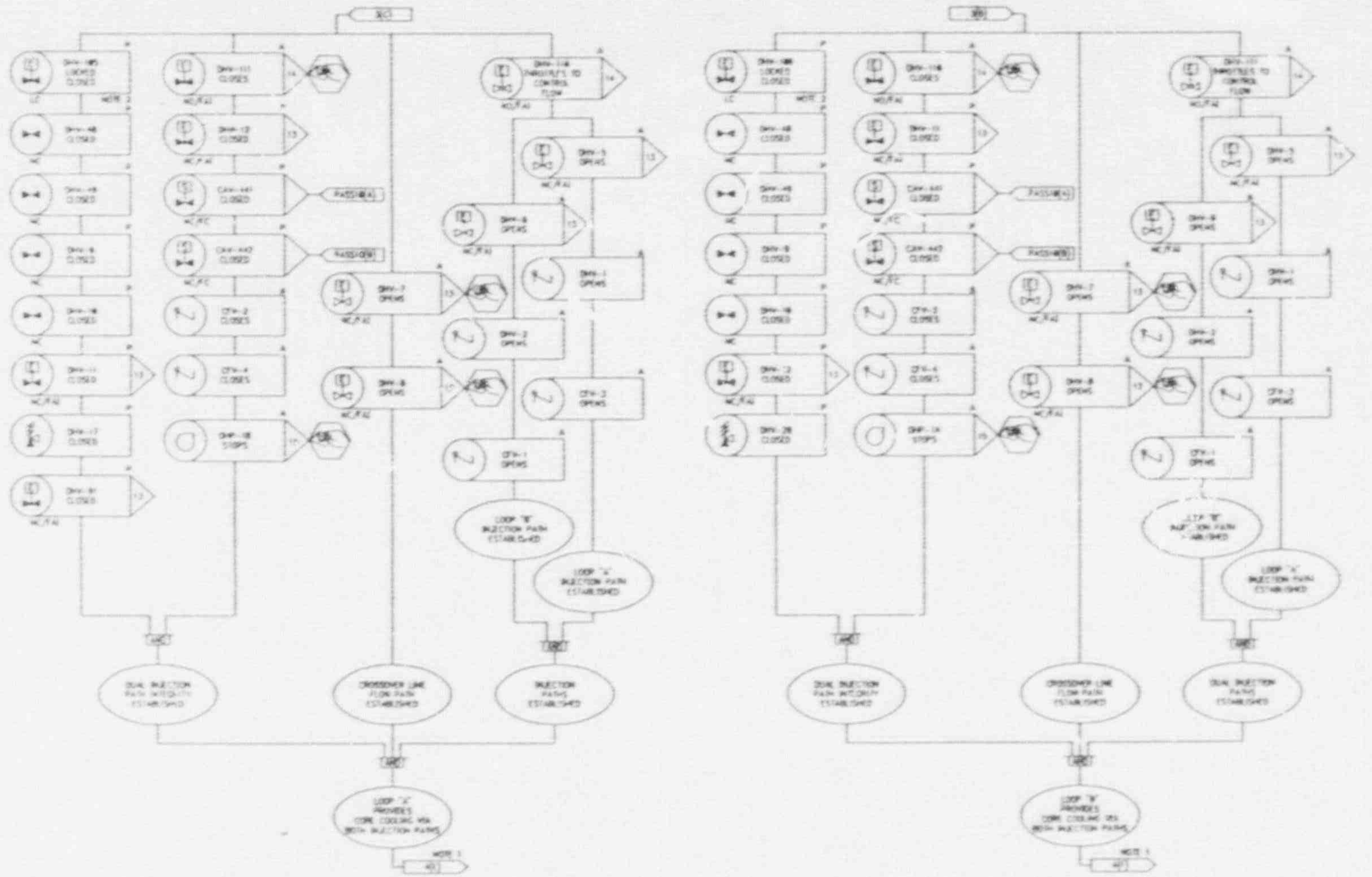
FLORIDA POWER CORPORATION
ST. PETERSBURG, FLORIDA
CRYSTAL RIVER PLANT
UNIT NO 3 855,928 KW

SAFETY FUNCTION DIAGRAM
DECAY HEAT REMOVAL
LPI LONG TERM COOLING MODE (SINGLE LOOP)
COMPOSITE

IMPELL

DRAWN BY LWR DATE
CHECKED BY JBH DATE
APPROVED BY DATE

SCALE | DRAWING NUMBER 0920-136-DH | SHEET 4 OF 5 | REV B



PRELIMINARY
FOR INFORMATION ONLY

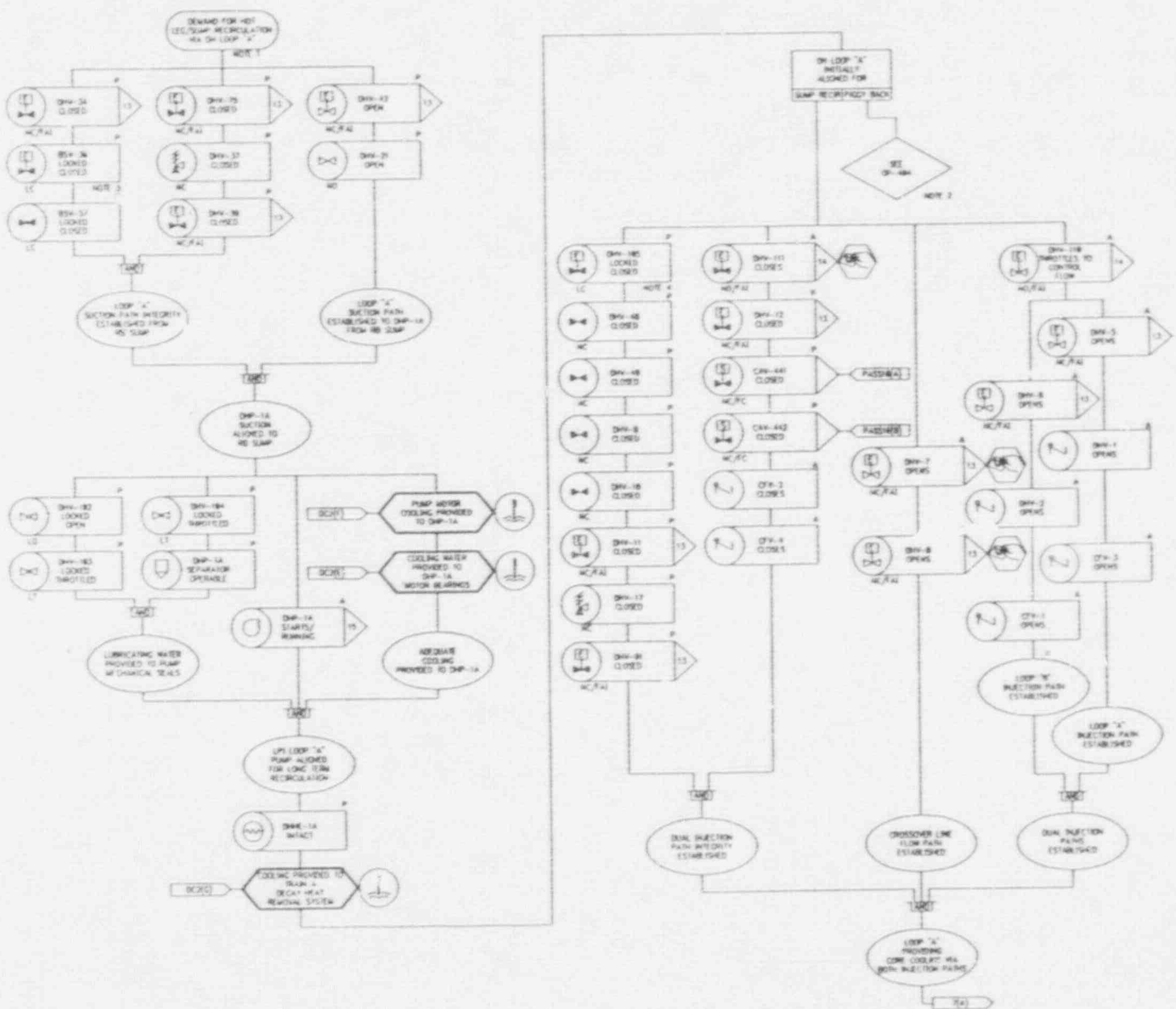
NO	REVISIONS	BY	CHECKED	APPROVED	DATE

FLORIDA POWER CORPORATION
ST. PETERSBURG, FLORIDA
CRYSTAL RIVER PLANT
UNIT NO 3

SAFETY FUNCTION DIAGRAM
DECAY HEAT REMOVAL
LPI LONG TERM COOLING MODE (DUAL LOOP)
COMPOSITE

IMPELL

0920-136-DH
SCALE | DRAWING NUMBER



NOTES:

1. THE BORON PRECIPITATION MODE OF DH SYSTEM OPERATION MUST BE ALIGNED WITHIN [illegible] HOURS AFTER A LARGE BREAK LOCA TO PREVENT THE DEVELOPMENT OF CORE FLOW BLOCKAGE WHICH MAY RESULT FROM EVAPORATION WITHIN THE REACTOR VESSEL. THE INITIAL CONDITION FOR THIS MODE OF OPERATION IS THE LOW PRESSURE INJECTION SUMP RECIRCULATION MODE. THE FLOW PATH MODELED ON THIS SFD DEPICTS TRAIN A DH SYSTEM OPERATION, WITH DHP-1B SECURED.

2. IF THE DH SYSTEM IS OPERATING IN PIGGY BACK MODE, OP-404, "DECAY HEAT REMOVAL SYSTEM", PROVIDES A METHOD TO ESTABLISH DROP LINE FLOW TO PREVENT BORON PRECIPITATION. HOWEVER, THIS MODE OF BORON PRECIPITATION IS NOT REFERENCED IN THE B&W LOCA ANALYSIS [illegible] AND IS, THEREFORE, NOT CONSIDERED ESSENTIAL. ADDITIONALLY, BORON PRECIPITATION IS ONLY A SIGNIFICANT CONCERN FOLLOWING RCS BREAKS WHICH ARE LARGE ENOUGH TO ALLOW THE REACTOR VESSEL TO ACT AS AN EVAPORATOR. THUS, THE PIGGY BACK MODE OF DH SYSTEM OPERATION WILL NOT BE REQUIRED, SINCE RCS DEPRESSURIZATION WILL ALLOW SUFFICIENT LPI FLOW.

3. NORMALLY LOCKED CLOSED BY HANDWHEEL AND BY POWER REMOVED.

4. NORMALLY LOCKED CLOSED BY POWER REMOVED.

PRELIMINARY
FOR INFORMATION ONLY
THIS DIAGRAM REFLECTS PLANT CONFIGURATION AS OF AUGUST 8, 1989

NO.	REVISIONS	BY	CHECKED	APPROVED	DATE

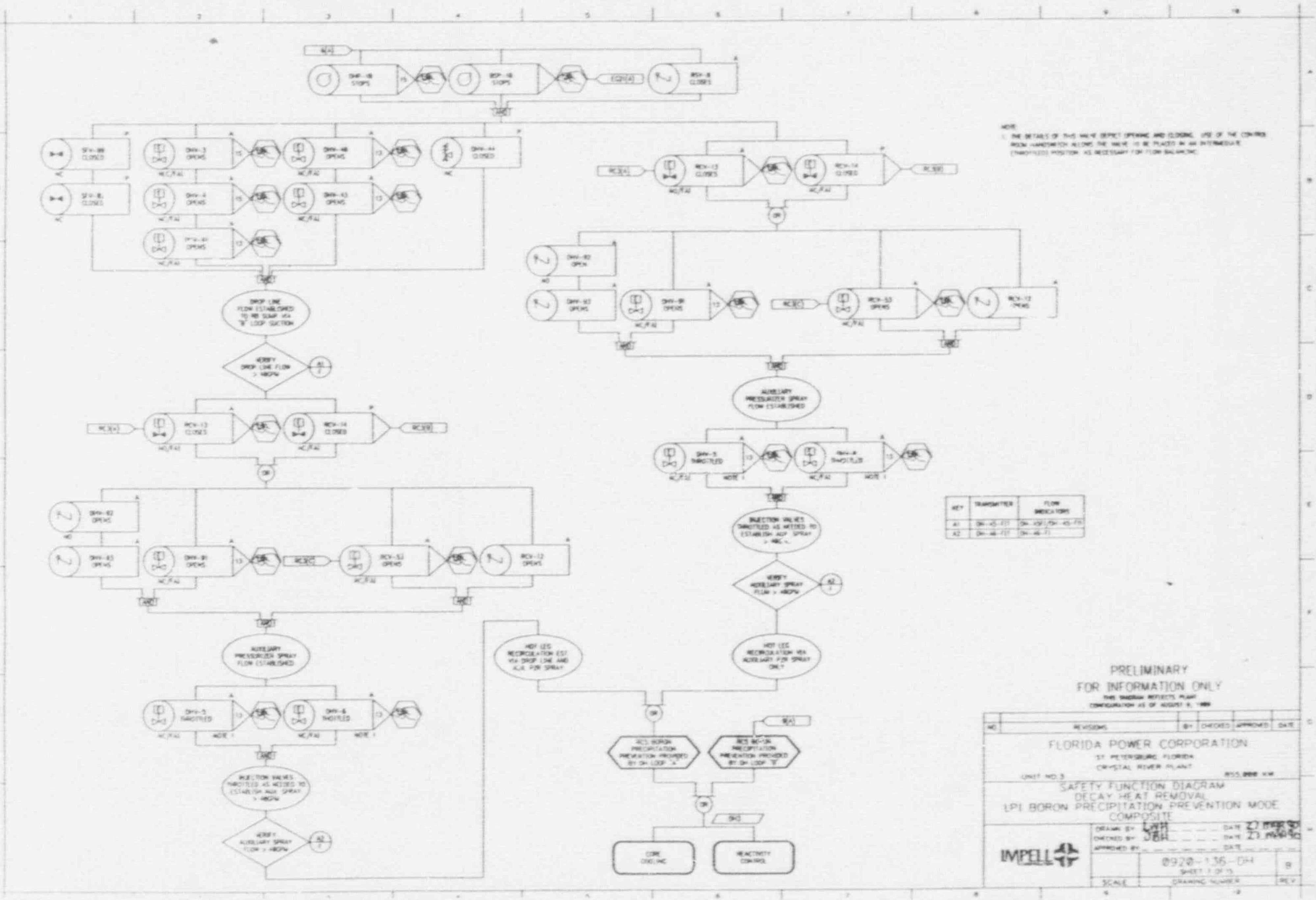
FLORIDA POWER CORPORATION
ST. PETERSBURG, FLORIDA
CRYSTAL RIVER PLANT
UNIT NO. 3 — 851,000 KW

SAFETY FUNCTION DIAGRAM
DECAY HEAT REMOVAL
LPI BORON PRECIPITATION PREVENTION MODE
COMPOSITE

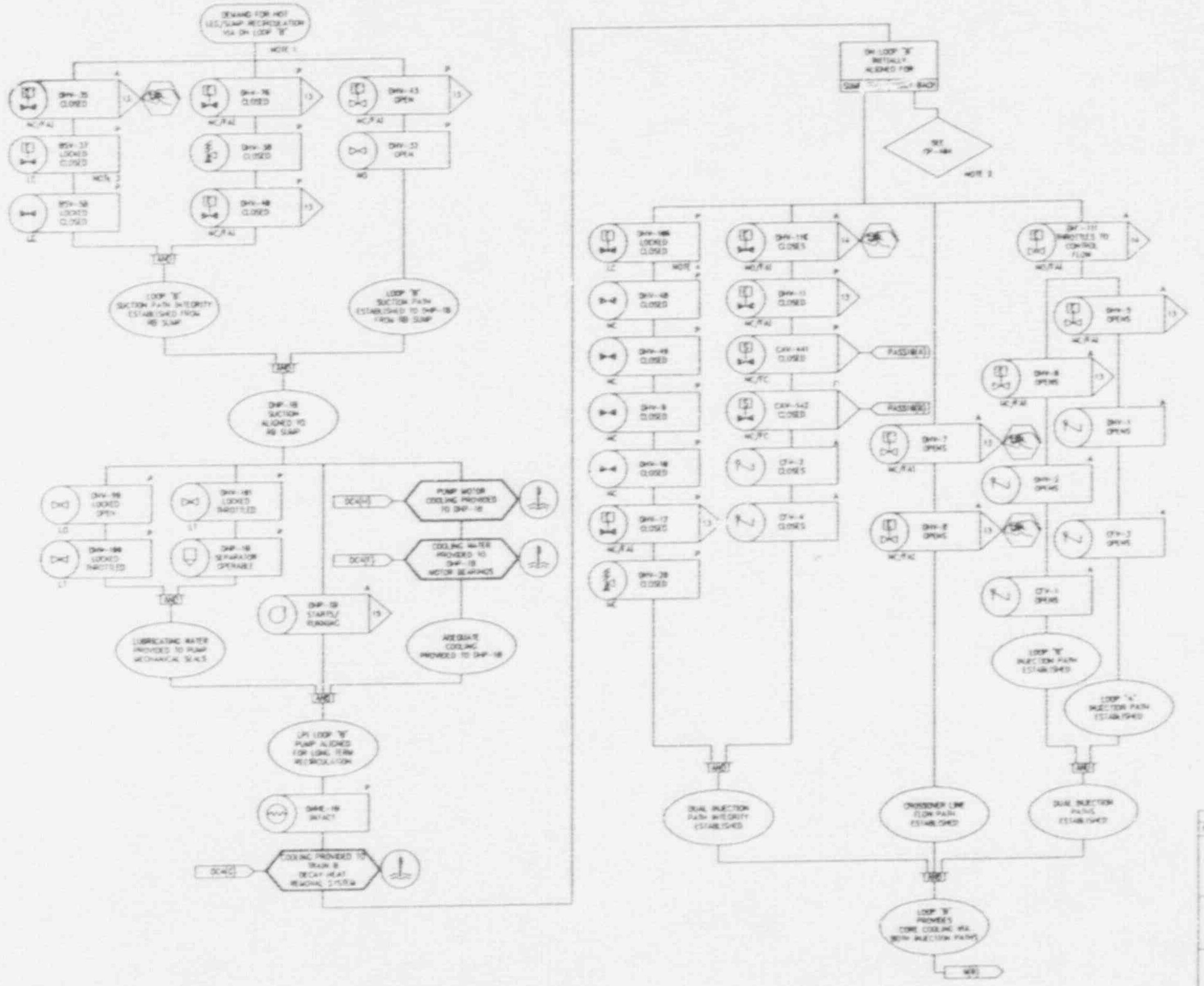
IMPELL

DRAWN BY: LWH DATE: 21 MAR 90
CHECKED BY: JBH DATE: 21 MAR 90
APPROVED BY: DATE:

SCALE — 0920-136-DH — SHEET 8 OF 13 — DRAWING NUMBER — REV. 9



DROP LINE FLOW ESTABLISHED TO RB SUMP VIA "B" LOOP SUCTION
AUXILIARY PRESSURIZER SPRAY FLOW ESTABLISHED
HOT LEG RECIRCULATION VIA AUXILIARY PZR SPRAY ONLY
CORE COOLING
REACTIVITY CONTROL
PRELIMINARY
FOR INFORMATION ONLY
FLORIDA POWER CORPORATION
ST PETERSBURG, FLORIDA
CRYSTAL RIVER PLANT
UNIT NO.3
SAFETY FUNCTION DIAGRAM
DECAY HEAT REMOVAL
LPI BORON PRECIPITATION PREVENTION MODE
COMPOSITE
IMPELL
0920-136-DH



NOTES:

1. THE BORON PRECIPITATION MODE OF DH SYSTEM OPERATION MUST BE ALIGNED WITHIN 24 HOURS AFTER A LARGE BREAK LOCA TO PREVENT THE DEVELOPMENT OF CORE FLOW BLOCKAGE WHICH MAY RESULT FROM EVAPORATION WITHIN THE REACTOR VESSEL. THE INITIAL CONDITION FOR THIS MODE OF OPERATION IS THE LOW PRESSURE INJECTION SUMP RECIRCULATION MODE. THE FLOWPATH MODELED ON THIS SFD DEPICTS TRAIN B DH SYSTEM OPERATION, WITH DHP-1A SECURED.
2. IF THE DH SYSTEM IS OPERATING IN PIGGY BACK MODE, OP-404, "DECAY HEAT REMOVAL SYSTEM", PROVIDES A METHOD TO ESTABLISH DROP LINE FLOW TO PREVENT BORON PRECIPITATION. HOWEVER, THIS MODE OF BORON PRECIPITATION IS NOT REFERENCED IN THE B&W LOCA ANALYSIS (BAW-[illegible]), AND IS, THEREFORE, NOT CONSIDERED ESSENTIAL. ADDITIONALLY, BORON PRECIPITATION IS ONLY A SIGNIFICANT CONCERN FOLLOWING RCS BREAKS WHICH ARE LARGE ENOUGH TO ALLOW THE REACTOR VESSEL TO ACT AS AN EVAPORATOR. THUS, THE PIGGY BACK MODE OF DH SYSTEM OPERATION WILL NOT BE REQUIRED SINCE RCS DEPRESSURIZATION WILL ALLOW SUFFICIENT LPI FLOW.
3. NORMALLY LOCKED CLOSED BY HANDWHEEL AND BY POWER REMOVED.
4. NORMALLY LOCKED CLOSED BY POWER REMOVED.

PRELIMINARY
FOR INFORMATION ONLY

NO.	REVISIONS	BY	CHECKED	APPROVED	DATE

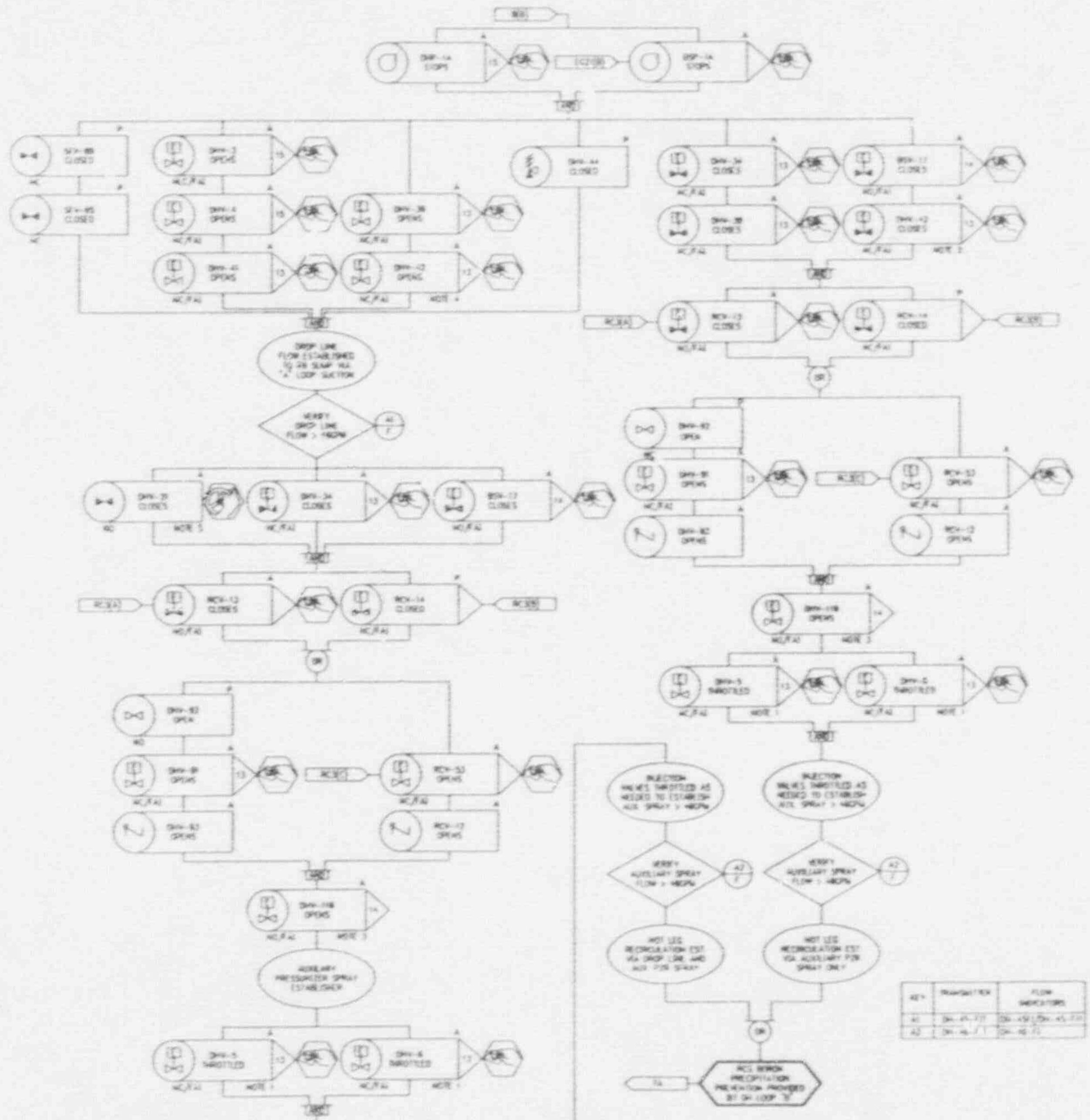
FLORIDA POWER CORPORATION
ST. PETERSBURG, FLORIDA
CRYSTAL RIVER PLANT
UNIT NO. 3

SAFETY FUNCTION DIAGRAM
DECAY HEAT REMOVAL
LPI BORON PRECIPITATION PREVENTION MODE
COMPOSITE

IMPELL

DRAWN BY — DATE
CHECKED BY — DATE
APPROVED BY — DATE

0920-136-DH — REV. B
SCALE — DRAWING NUMBER



NOTES:

1. THE DETAILS OF THIS VALVE DEPICT OPENING AND CLOSING. USE OF THE CONTROL ROOM HANDSWITCH ALLOWS THE VALVE TO BE PLACED IN AN INTERMEDIATE (THROTTLED) POSITION, AS NECESSARY FOR FLOW BALANCING.
2. THIS VALVE IS NORMALLY CLOSED, BUT MAY HAVE BEEN OPENED PREVIOUSLY TO ESTABLISH DH LOOP "A" LPI RECIRCULATION MODE OF OPERATION.
3. THIS VALVE WAS PREVIOUSLY CLOSED TO PREVENT BACKFLOW THROUGH THE IDLE DH PUMP. OPENING THIS VALVE ESTABLISHES THE FLOWPATH NEEDED FOR AUXILIARY SPRAY FLOW.
4. AN APPARENT ERROR WAS IDENTIFIED IN OP-404, STEP [illegible]. THIS STEP DIRECTS THE OPERATOR TO CLOSE DHV-42. HOWEVER, THIS ACTION WOULD TERMINATE FLOW FROM THE DROP LINE TO THE RB SUMP. THIS ACTION IS CONTRARY TO THE PRECEDING STEPS WHICH ALIGN THE DROP LINE TO THE RB SUMP.
5. DHV-21 IS A MANUAL VALVE WHICH MUST BE LOCALLY CLOSED.

PRELIMINARY
FOR INFORMATION ONLY
THIS DIAGRAM REFLECTS PLANT CONFIGURATION AS OF AUGUST 8, 1988

NO.	REVISIONS	BY	CHECKED	APPROVED	DATE

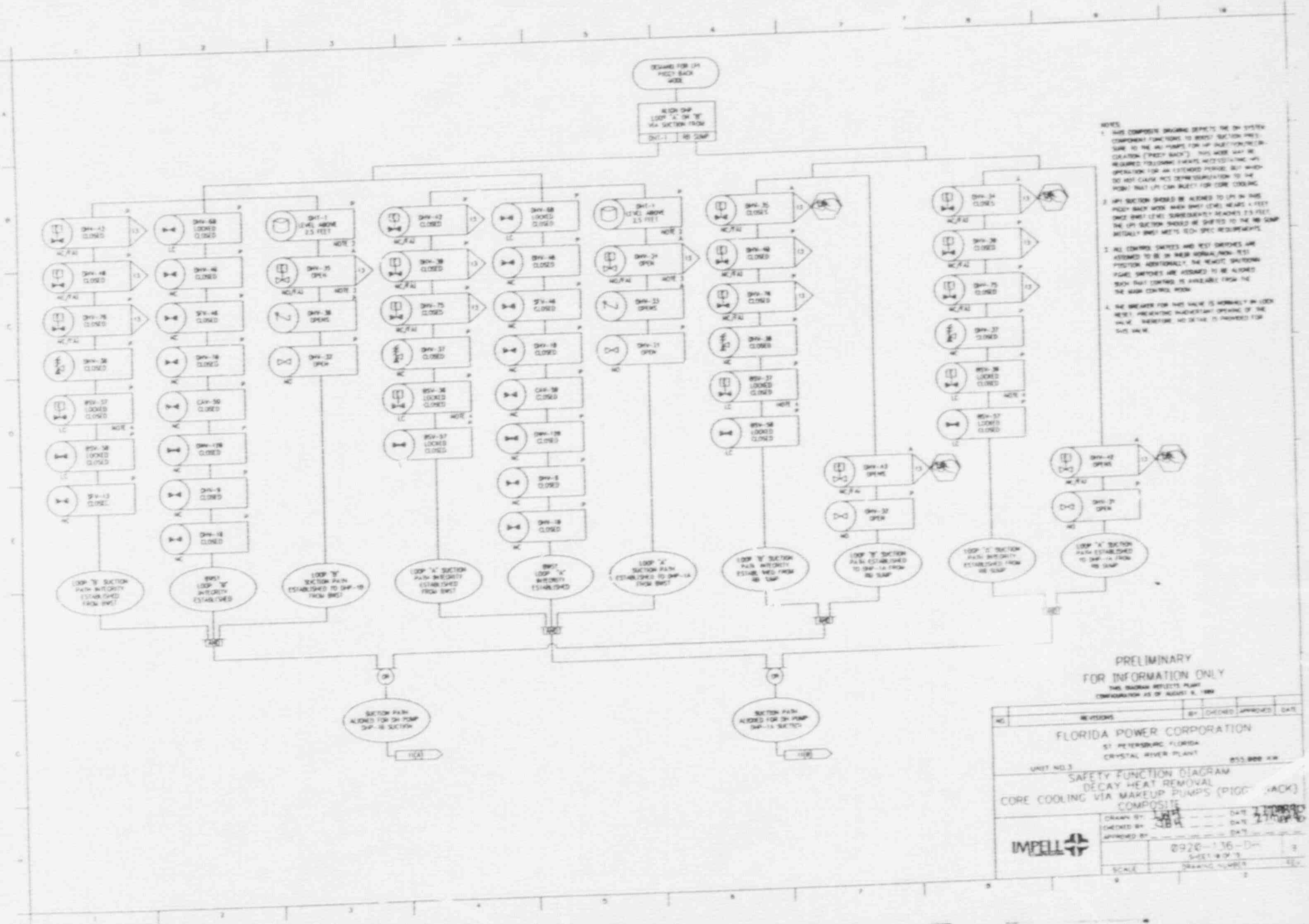
FLORIDA POWER CORPORATION
ST. PETERSBURG, FLORIDA
CRYSTAL RIVER PLANT
UNIT NO. 3 855,000 KW

SAFETY FUNCTION DIAGRAM
DECAY HEAT REMOVAL
LPI BORON PRECIPITATION PREVENTION MODE
COMPOSITE

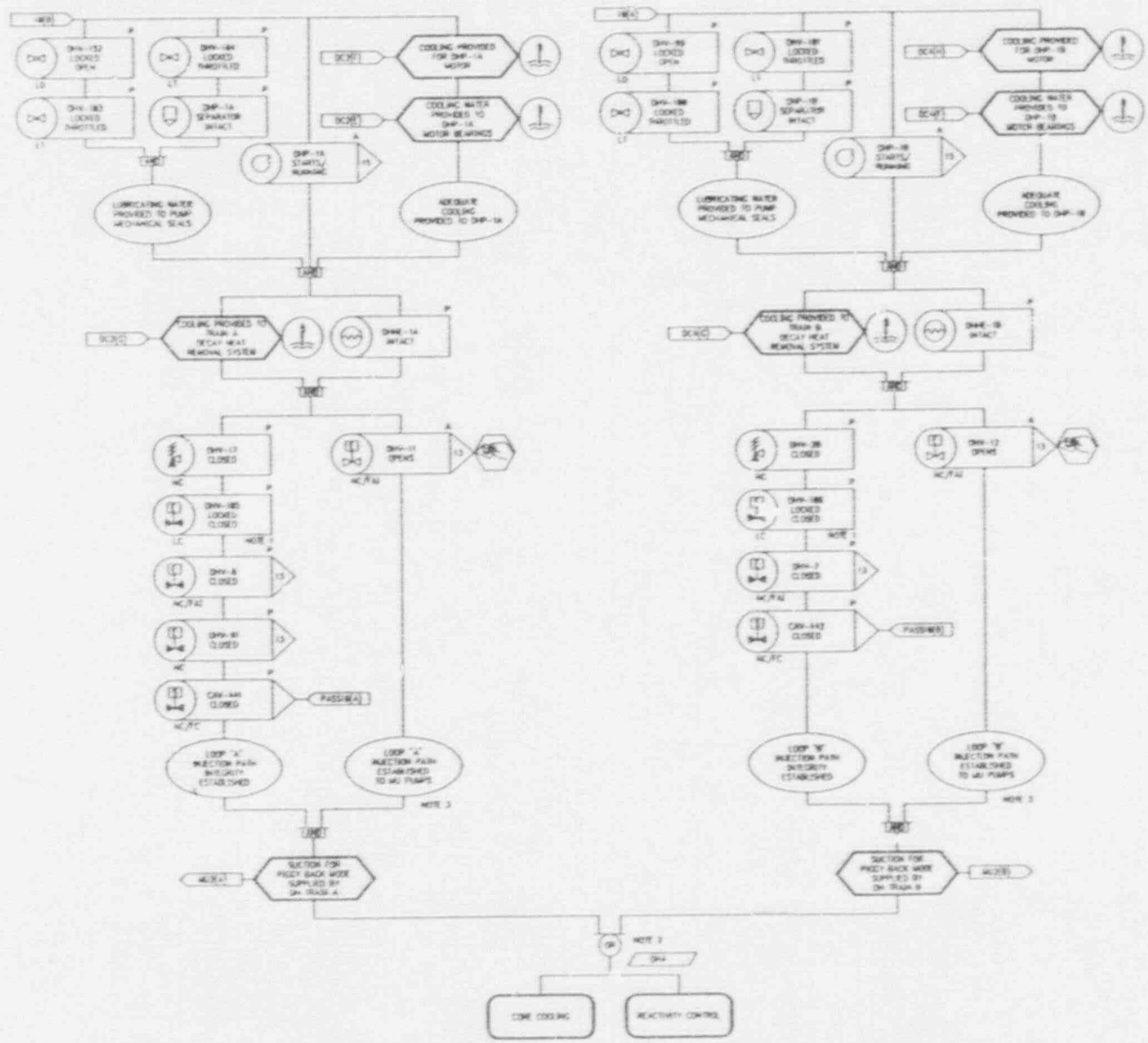
IMPELL

DRAWN BY LHM DATE 27 MAR 90
CHECKED BY JBH DATE 27 MAR 90
APPROVED BY DATE

0928-136-D-4 SHEET 4 OF 5 — REV 0
SCALE — DRAWING NUMBER — REV



PRELIMINARY
FOR INFORMATION ONLY
FLORIDA POWER CORPORATION
ST. PETERSBURG, FLORIDA
CRYSTAL RIVER PLANT
UNIT NO.3
SAFETY FUNCTION DIAGRAM
DECAY HEAT REMOVAL
CORE COOLING VIA MAKEUP PUMPS (PIGGY BACK)
COMPOSITE
IMPELL



NOTES:

1. THE BREAKER FOR THIS VALVE IS NORMALLY IN LOCK RESET, PREVENTING INADVERTANT OPENING OF THE VALVE. THEREFORE, NO DETAIL IS PROVIDED FOR THIS VALVE.
2. ONE DH PUMP IS CAPABLE OF PROVIDING SUFFICIENT FLOW TO BOTH MAKEUP PUMPS WHILE HPI IS REQUIRED. HOWEVER, THE MAKEUP PUMP SUCTION CROSS-CONNECT VALVES (MUV-62, -63, -68, -69) MUST BE OPEN TO ALLOW ONE DH TRAIN TO FEED ALL MAKEUP PUMPS.
3. WHILE PROVIDING FLOW TO THE HPI PUMPS, THE DH PUMPS MUST BE MONITORED TO PREVENT PUMP RUNOUT SINCE THE FLOW ELEMENTS WHICH CONTROL THROTTLE VALVE POSITION (DHV-110, -111) DO NOT MEASURE DH SYSTEM FLOW WHICH IS DIRECTED TO THE HPI PUMPS. THE FLOW CONTROL VALVES AND LPI INJECTION VALVES (DHV-5, -6) ARE NOT SHOWN HERE SINCE THEIR POSITION IS NOT CRITICAL TO THE PIGGY BACK MODE OF OPERATION.

PRELIMINARY
FOR INFORMATION ONLY
THIS DIAGRAM REFLECTS PLANT CONFIGURATION AS OF AUGUST 6, 1989

NO.	REVISIONS	BY	CHECKED	APPROVED	DATE

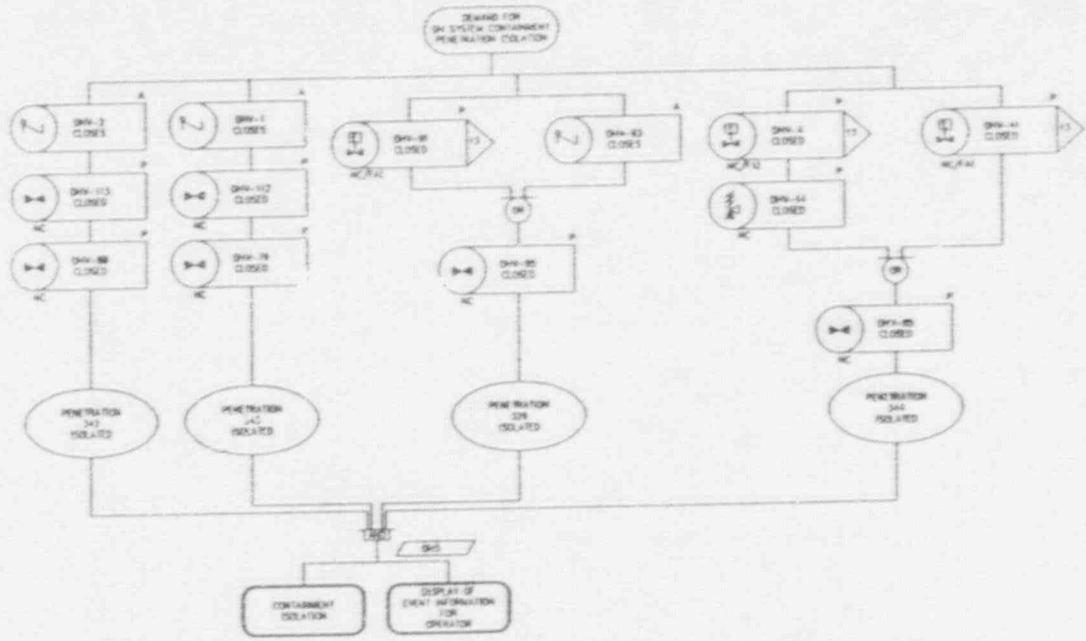
FLORIDA POWER CORPORATION
ST. PETERSBURG, FLORIDA
CRYSTAL RIVER PLANT
UNIT NO.3 855,000 KW

SAFETY FUNCTION DIAGRAM
DECAY HEAT REMOVAL
CORE COOLING VIA MAKEUP PUMPS (PIGGY BACK)
COMPOSITE

IMPELL

DRAWN BY LWH DATE 21 MAR 90
CHECKED BY JEA DATE 21 MAR 90
APPROVED BY DATE

SCALE | DRAWING NUMBER 0920-136-DH SHEET 11 OF 15 | REV. B



PRELIMINARY
FOR INFORMATION ONLY

NO	REVISIONS	BY	CHECKED	APPROVED	DATE

FLORIDA POWER CORPORATION

CRYSTAL RIVER PLANT

UNIT NO. 3

DELAY HEAT REMOVAL
SAFTEY FUNCTION DIAGRAM
COMPOSITE

IMPELL

DRAWN BY
CHECKED BY
APPROVED BY

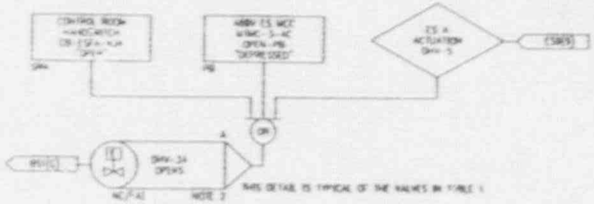
DATE
DATE
DATE

SCALE

0920-136-DH

DRAWING NUMBER

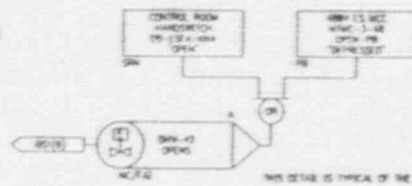
REV. B



THIS DETAIL IS TYPICAL OF THE VALVES IN TABLE 1.

TABLE 1

VALVE	C.R. HANDSWITCH	4BBV ES MCC PB	ES ACTUATION	TRANSFER FLAGS		COMPOSITE SHEET
DHV-34	CB-ESFA-KJ4	MTMC-3-4C	ES A DHV-34	ESB(5)	BSI(C)	1, 10
DHV-6	CB-ESFB-KP4	MTMC-5-9C	ES B DHV-6	ESB(R)	------	2, 4, 5, 6, 7, 8, 9
DHV-5	CB-ESFA-KP4	MTMC-3-1C	ES A DHV-5	ESB(Q)	------	2, 4, 5, 6, 7, 8, 9
DHV-35	CB-ESFB-KJ4	MTMC-5-6B	ES B DHV-35	ESB(T)	BSI(W)	1, 10

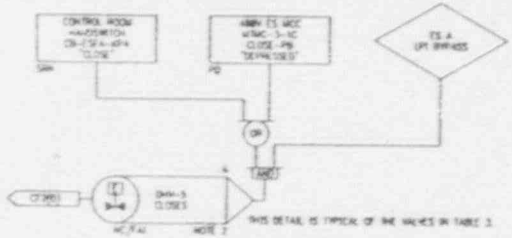


THIS DETAIL IS TYPICAL OF THE VALVES IN TABLE 2.

TABLE 2

VALVE	C.R. HANDSWITCH	4BBV ES MCC PB	TRANSFER FLAGS	COMPOSITE SHEET
DHV-42	CB-ESFA-KH4	MTMC-3-4B	BSI(B)	3, 6, 9
DHV-12	CB-ESFB-KH4	MTMC-5-5A	------	6, 11
DHV-41	CB-ESFB-KG4	MTMC-3-4C	------	7, 8
DHV-11	CB-ESFA-KH4	MTMC-3-7A	------	11
DHV-43	CB-ESFB-KH4	MTMC-5-6A	BSI(J)	3, 7, 8, 10
DHV-91	CB-ESFAB-ELV	MTMC-7-5C	------	7, 8
DHV-7	CB-ESFB-TA4	MTMC-7-6AL	------	5, 6, 8, 11
DHV-8	CB-ESFA-TA4	MTMC-7-6AR	------	3, 4, 8
DHV-38	CB-ESFA-TC4	MTMC-3-8C	------	9
DHV-48	CB-ESFB-TC4	MTMC-5-8C	------	7

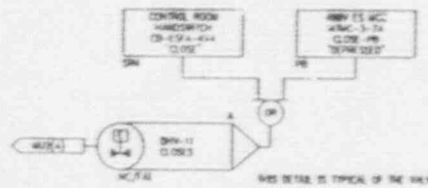
NOTE 3



THIS DETAIL IS TYPICAL OF THE VALVES IN TABLE 3.

TABLE 3

VALVE	C.R. HANDSWITCH	4BBV ES MCC PB	ES ACTUATION	TRANSFER FLAGS	COMPOSITE SHEET
DHV-5	CB-ESFA-KP4	MTMC-3-1C	ES A LPI BYPASS	CF2(B)	7, 9, 12
DHV-6	CB-ESFB-KP4	MTMC-5-9C	ES B LPI BYPASS	CF1(C)	7, 9, 12
DHV-34	CB-ESFA-KJ4	MTMC-3-4C	ES A LPI BYPASS	BSI(C)	3, 6, 9, 10
DHV-35	CB-ESFB-KJ4	MTMC-5-6B	ES B LPI BYPASS	BSI(K)	3, 8, 10

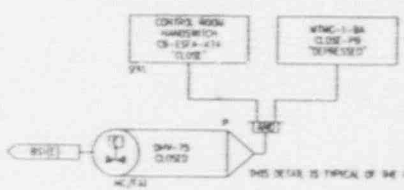


THIS DETAIL IS TYPICAL OF THE VALVES IN TABLE 4.

TABLE 4

VALVE	C.R. HANDSWITCH	4BBV ES MCC PB	TRANSFER FLAGS	COMPOSITE SHEET
DHV-11	CB-ESFA-KH4	MTMC-3-7A	WUX(A)	2, 4, 5, 6, 8
DHV-12	CB-ESFB-KH4	MTMC-5-5A	WUX(C)	2, 4, 5, 8
DHV-42	CB-ESFA-KH4	MTMC-3-4B	BSI(F)	1, 8, 10, 12
DHV-43	CB-ESFB-KH4	MTMC-5-6A	BSI(L)	1, 10, 12
DHV-91	CB-ESFAB-ELV	MTMC-7-5C	------	2, 4, 5, 6, 11, 12
DHV-7	CB-ESFB-TA4	MTMC-7-6AL	------	2, 4, 6, 11
DHV-8	CB-ESFA-TA4	MTMC-7-6AR	------	2, 4, 6, 11
DHV-38	CB-ESFA-TC4	MTMC-3-8C	BSI(J)	1, 3, 6, 9
DHV-48	CB-ESFB-TC4	MTMC-5-6C	BSI(H)	1, 3, 8, 10

NOTE 3



THIS DETAIL IS TYPICAL OF THE VALVES IN TABLE 5.

TABLE 5

VALVE	C.R. HANDSWITCH	MCC & UNIT	TRANSFER FLAGS	COMPOSITE SHEET
DHV-75	CB-ESFA-KT4	MTMC-1-8A	BSI(E)	1, 3, 6, 10
DHV-76	CB-ESFB-KT4	MTMC-2-7B	BSI(I)	1, 3, 8, 10
DHV-41	CB-ESFB-KG4	MTMC-7-4C	------	12

NOTE 3

NOTES

1. ALL CONTROL SWITCHES AND TEST SWITCHES ARE ASSUMED TO BE IN THEIR NORMAL/NON-TEST POSITION. ADDITIONALLY, THE REMOTE SHUTDOWN PANEL SWITCHES ARE ASSUMED TO BE ALIGNED SUCH THAT CONTROL IS AVAILABLE FROM THE MAIN CONTROL ROOM.
2. DH INJECTION VALVES DHV-5 AND DHV-6 MAY ALSO BE REQUIRED IN AN INTERMEDIATE/THROTTLED POSITION IN ORDER TO BALANCE LPI FLOWS. AFTER A BYPASS OF THE ES LPI ACTUATION SIGNAL, THESE VALVES MAY BE JOGGED INTO THE DESIRED POSITION USING THE APPROPRIATE HANDSWITCHES.
3. EACH OF THESE VALVES STROKES FULLY CLOSED AFTER THE HANDSWITCH IS MOMENTARILY TAKEN TO THE "CLOSE" POSITION. HOWEVER, DURING PREPARATION OF THESE DETAILS IT WAS NOTED THAT THE VALVE CLOSING CIRCUIT IS ONLY DEENERGIZED BY ACTUATION OF THE CLOSING TORQUE LIMIT SWITCH.

PRELIMINARY
FOR INFORMATION ONLY
THIS DIAGRAM REFLECTS PLANT
CONFIGURATION AS OF AUGUST 8, 1989

NO	REVISIONS	BY	CHECKED	APPROVED	DATE

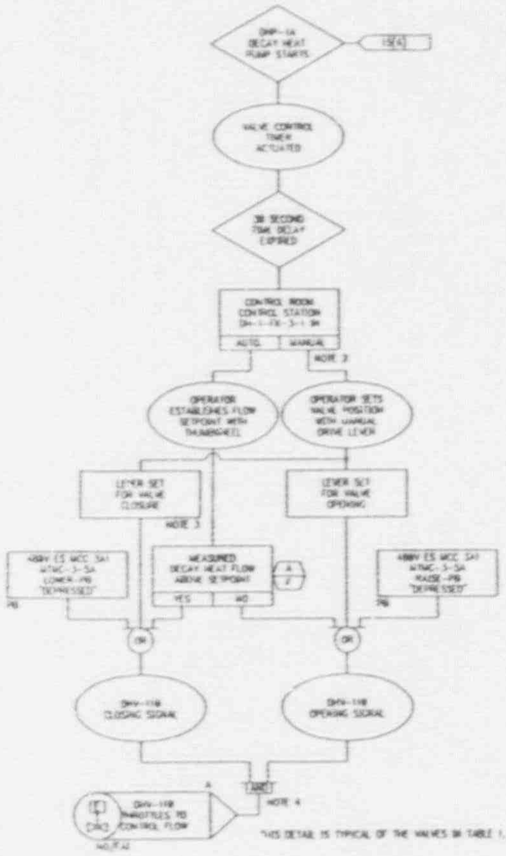
FLORIDA POWER CORPORATION
ST. PETERSBURG, FLORIDA
CRYSTAL RIVER PLANT
UNIT NO. 3 — 855,000 KW

SAFETY FUNCTION DIAGRAM
DECAY HEAT REMOVAL
DETAILS

IMPELL

DRAWN BY LWH DATE 27MAR90
CHECKED BY JBH DATE 27MAR90
APPROVED BY ---- DATE ----

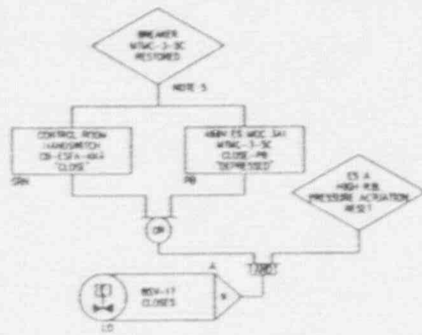
0920-136-DH
SHEET 13 OF 15
DRAWING NUMBER
SCALE
REV 0

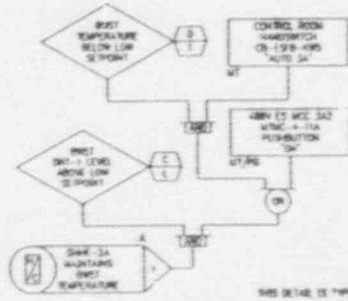


THIS DETAIL IS TYPICAL OF THE VALVES IN TABLE 1.

TABLE 1

VALVE	PUMP	CONTROL STATION	480V ES MCC UNIT	KEY	FLOW TRANSMITTER	COMPOSITE SHEET
DHV-110	DHP-1A	DH-1-FK-3-1	MTMC-3-5A	A	DH-1-FT3	2, 4, 5, 6, 8, 9
DHV-111	DHP-1B	DH-1-FK-4-1	MTMC-5-5B	B	DH-1-FT4	2, 4, 5, 7





THIS DETAIL IS TYPICAL OF THE HEATERS IN TABLE 2.

TABLE 2

HEATER	KEY	LEVEL SWITCH	KEY	TEMPERATURE SWITCH	CB HANDSWITCH/POSITION	480V MCC	COMPOSITE SHEET
DHHE-2A	C	DH-19-LS	D	DH-14-TTS	CB-ESFB-KW5/AUTO 3A	3A2/MTMC-4-11A	1
DHHE-2B	E	DH-19-LS	F	DH-9-TTS	CB-ESFB-KW5/AUTO 3B	3B2/MTMC-6-5D	1

NOTES:

1. ALL CONTROL SWITCHES AND TEST SWITCHES ARE ASSUMED TO BE IN THEIR NORMAL/NON-TEST POSITION. ADDITIONALLY, THE REMOTE SHUTDOWN PANEL SWITCHES ARE ASSUMED TO BE ALIGNED SUCH THAT CONTROL IS AVAILABLE FROM THE MAIN CONTROL ROOM.
2. THE DH FLOW CONTROL STATION IS NORMALLY MAINTAINED IN AUTOMATIC MODE WITH A FLOW SETPOINT OF 3000 GPM. TO THROTTLE FLOW, THE MANUAL PUSHBUTTON MUST BE DEPRESSED AND THE VALVE CONTROL LEVER ON THE CONTROL STATION MOVED TO ESTABLISH THE DESIRED VALVE POSITION.
3. THE HOT LEG RECIRCULATION MODE OF DH OPERATION MAY NECESSITATE FULL CLOSURE OF THIS VALVE. A SEPARATE DETAIL IS NOT PROVIDED FOR FULL CLOSURE SINCE THIS CONDITION WOULD BE ESTABLISHED BY MANUAL VALVE CONTROL WITH THIS LEVER.
4. THIS "AND" GATE INDICATES THAT BOTH OPENING AND CLOSING SIGNALS ARE REQUIRED FOR FLOW CONTROL, BUT DOES NOT IMPLY THAT THE SIGNALS MUST BE RECEIVED CONCURRENTLY.
5. THIS BREAKER IS NORMALLY IN LOCK-RESET TO PREVENT INADVERTENT CLOSURE OF BSV-17. IT MUST BE LOCALLY RESET PRIOR TO REMOTE VALVE OPERATION.

PRELIMINARY
FOR INFORMATION ONLY
THIS DIAGRAM REFLECTS PLANT CONFIGURATION AS OF AUGUST 8, 1989

NO.	REVISIONS	BY	CHECKED	APPROVED	DATE

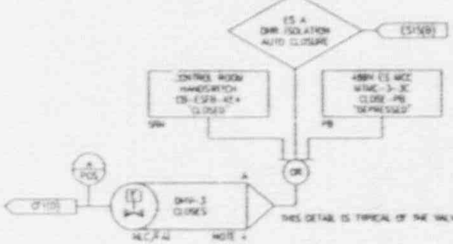
FLORIDA POWER CORPORATION
ST. PETERSBURG, FLORIDA
CRYSTAL RIVER PLANT
UNIT NO.3 — 755 MW

SAFETY FUNCTION DIAGRAM
DECAY HEAT SYSTEM
DETAIL

IMPELL

DRAWN BY: LWH DATE: 21 MAR 90
CHECKED BY: JBH DATE: 21 MAR 90
APPROVED BY: DATE:

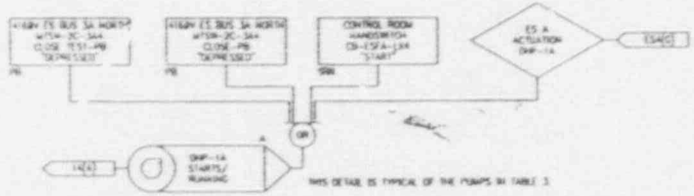
0920-136-DH — SHEET 14 OF 15 — REV. B
SCALE — DRAWING NUMBER



THIS DETAIL IS TYPICAL OF THE VALVES IN TABLE 2

TABLE 2

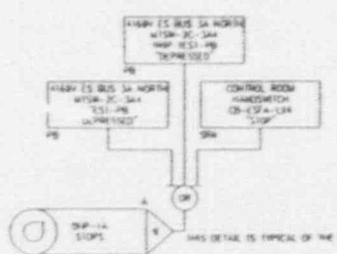
VALVE	C.R. HANDSWITCH	480V ES MCC UNIT	ES TRANSFER FLAGS	RC SFD	KEY	LIMIT SWITCH	TRANSFER FLAGS
DHV-3	CB-ESFB-KE4	MTMC-3-3C	ES15(B) CF1(D)	RC2(A)	A	DHV-3-25	CF1(D)
DHV-4	CB-ESFA-KF4	MTMC-5-11B	ES15(C) CF1(E)	RC1(B)	B	DHV-4-25	CF1(E)



THIS DETAIL IS TYPICAL OF THE PUMPS IN TABLE 3

TABLE 3

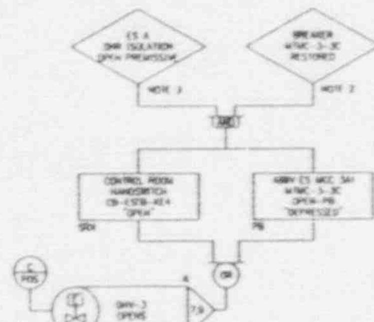
PUMP	ES BUS	SWITCHGEAR UNIT	CR HANDSWITCH	ES ACTUATION	TRANSFER FLAG	COMPOSITE SHEETS
DHP-1A	4160V 3A NORTH	MTSW-2C-3A4	CB-ESFA-LX4	ES A DHP-1A	ES4(C)	1, 2, 3, 6, 11
DHP-1B	4160V 3B NORTH	MTSW-2E-3B11	CB-ESFB-LX4	ES B DHP-1B	ES7(D)	1, 2, 3, 6, 11



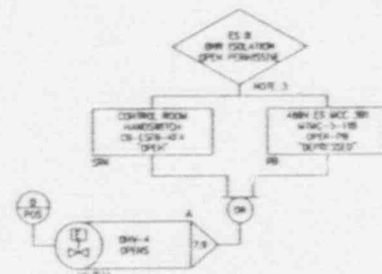
THIS DETAIL IS TYPICAL OF THE PUMPS IN TABLE 4.

TABLE 4

PUMP	ES BUS	SWITCHGEAR UNIT	CR HANDSWITCH	COMPOSITE SHEETS
DHP-1A	4160V 3A NORTH	MTSW-2C-3A4	CB-ESFA-LX4	6
DHP-1B	4160V 3B NORTH	MTSW-2E-3B11	CB-ESFB-LX4	7



KEY	LIMIT SWITCH
C	DHV-3-25



KEY	LIMIT SWITCH
D	DHV-4-25

NOTES

1. ALL CONTROL SWITCHES AND TEST SWITCHES ARE ASSUMED TO BE IN THEIR NORMAL/NON-TEST POSITION. ADDITIONALLY, THE REMOTE SHUTDOWN PANEL SWITCHES ARE ASSUMED TO BE ALIGNED SUCH THAT CONTROL IS AVAILABLE FROM THE MAIN CONTROL ROOM.
2. THIS BREAKER IS NORMALLY IN LOCK-RESET TO PREVENT INADVERTANT OPERATION OF DHV-3 WHICH COULD RESULT IN DH SYSTEM OVERPRESSURIZATION. IT MUST BE LOCALLY RESET PRIOR TO REMOTE OPERATION OF THE VALVE.
3. THIS PERMISSIVE IS ESTABLISHED BY THE SAME ACTUATION LOGIC WHICH AUTOMATICALLY CLOSES DHV-3 AND DHV-4 ON HIGH RCS PRESSURE. SINCE THE ES SFD MODELS ONLY ACTUATIONS, NO TRANSFER FLAG IS PROVIDED FOR THIS PERMISSIVE.
4. DHV-3 IS NORMALLY LOCKED CLOSED TO PREVENT INADVERTANT OPERATION OF THE VALVE RESULTING IN DH SYSTEM OVERPRESSURIZATION. THIS DETAIL IS PROVIDED SHOULD THIS VALVE NEED TO BE CLOSED TO SUPPORT RCS PRESSURE BOUNDARY INTEGRITY SAFETY FUNCTION OF THE RC SYSTEM SFD. DHV-4 ALSO SUPPORTS CORE FLOOD SYSTEM INTEGRITY AND PROVIDES VALVE POSITION INDICATION REQUIRED FOR POST-ACCIDENT MONITORING.

PRELIMINARY
FOR INFORMATION ONLY
THIS DIAGRAM REFLECTS PLANT CONFIGURATION AS OF AUGUST 8, 1989

NO.	REVISIONS	BY	CHECKED	APPROVED	DATE

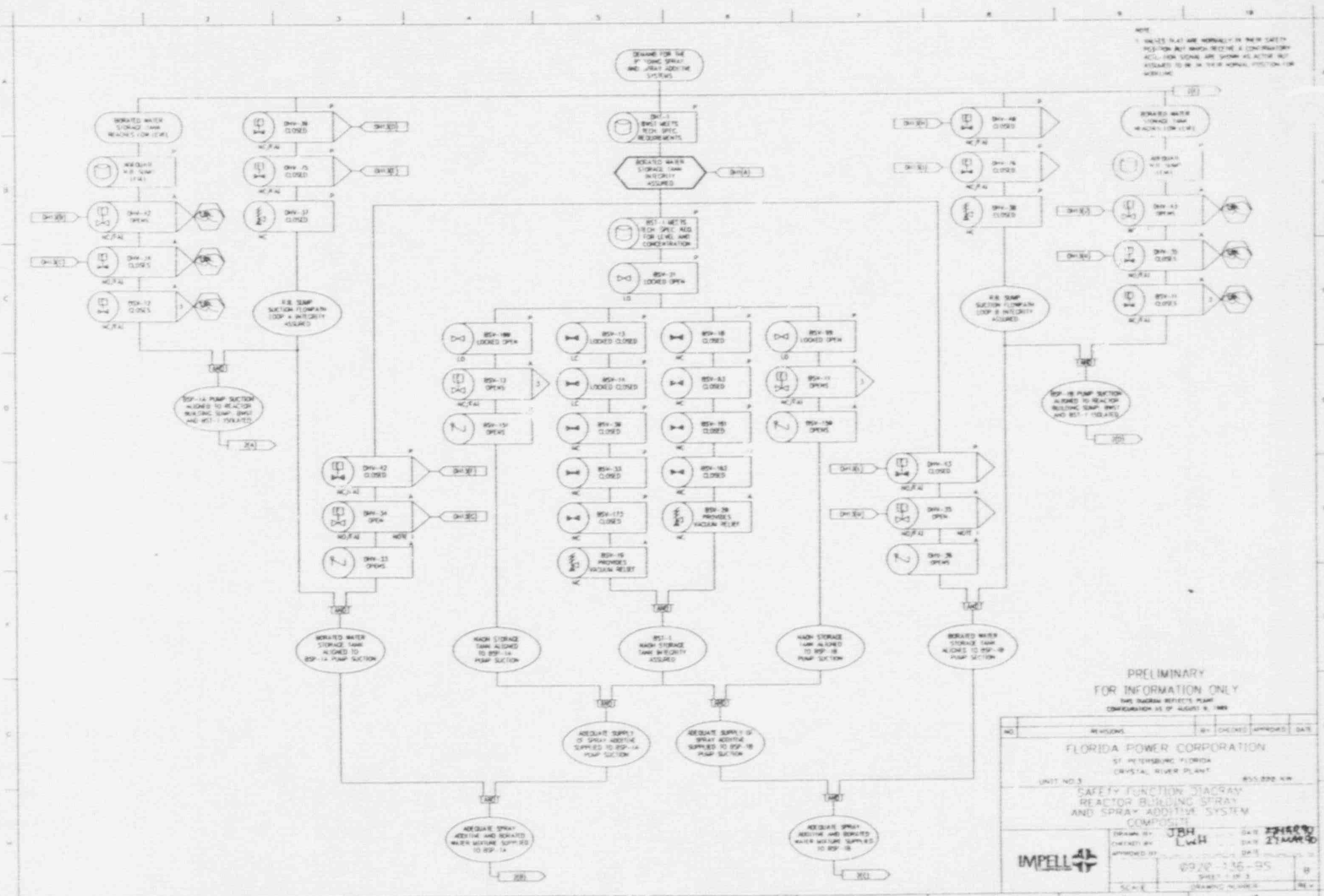
FLORIDA POWER CORPORATION
ST. PETERSBURG, FLORIDA
CRYSTAL RIVER PLANT
UNIT NO. 3 — 855,000 KW

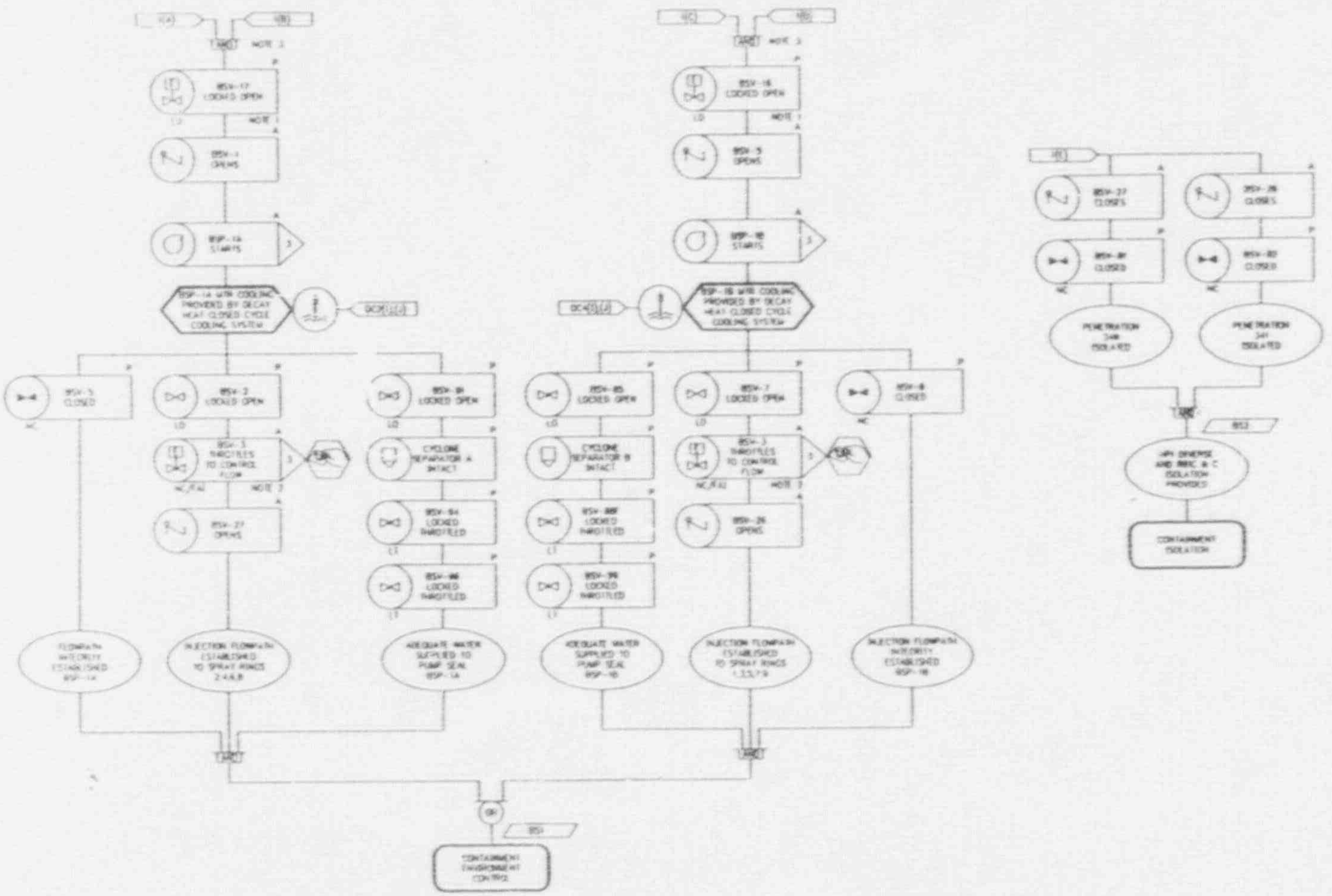
SAFETY FUNCTION DIAGRAM
DECAY HEAT REMOVAL
DETAILS

IMPELL

DRAWN BY LOH DATE 27MAR90
CHECKED BY DBH DATE 27MAR90
APPROVED BY ____ DATE ____

SCALE — 0920-136-DH — SHEET 15 OF 15 — DRAWING NUMBER — REV. B


PRELIMINARY
FOR INFORMATION ONLY
FLORIDA POWER CORPORATION
ST. PETERSBURG, FLORIDA
CRYSTAL RIVER PLANT
UNIT NO.3
SAFETY FUNCTION DIAGRAM
REACTOR BUILDING SPRAY
AND SPRAY ADDITIVE SYSTEM
COMPOSITE
IMPELL
JBH
LWH
0920-136-95



NOTES:

1. VALVE IS NORMALLY LOCKED OPEN BY POWER REMOVAL. THEREFORE NO DETAIL IS PROVIDED FOR THIS VALVE.
2. REDUCED NPSH WILL BE EXPERIENCED AFTER SHIFTING PUMP SUCTION TO THE RB SUMP. THEREFORE, MANUAL OPERATOR ACTION IS SHOWN SINCE ACTION MUST BE TAKEN TO THROTTLE THIS VALVE TO REDUCE SYSTEM FLOW ONCE SUMP LEVEL IS REACHED IN THE SUMP.
3. ALTHOUGH BOTH FLOWPATHS ARE NOT ESTABLISHED CONCURRENTLY THIS "AND" GATE INDICATES THAT BOTH PATHS ARE ESSENTIAL TO ACCOMPLISH THE RB SPRAY SYSTEM SAFETY FUNCTION.
4. THIS VALVE IS NORMALLY CLOSED BUT WAS ASSUMED TO BE IN ITS SAFETY POSITION FOR CONTROLLING R.B. SPRAY FLOW PRIOR TO BEING CLOSED BY OPERATOR ACTION. FOR THIS REASON IT IS SHOWN AS ACTIVE BUT FOR ALL OTHER EVENTS WHERE R.B. SPRAY IS NOT CALLED UPON TO OPERATE THIS VALVE WOULD BE PASSIVE.

PRELIMINARY
FOR INFORMATION ONLY
THIS DIAGRAM REFLECTS PLANT CONFIGURATION AS OF AUGUST 8, 1988

NO.	REVISIONS	BY	CHECKED	APPROVED	DATE

FLORIDA POWER CORPORATION
ST. PETERSBURG, FLORIDA
CRYSTAL RIVER PLANT
UNIT NO. 3

SAFETY FUNCTION DIAGRAM
REACTOR BUILDING SPRAY
AND SPRAY ADDITIVE SYSTEM
COMPOSITE

DRAWN BY: JBH DATE: 12MAR90
CHECKED BY: LWH DATE: 27MAR90
APPROVED BY: DATE:

IMPELL

0920-136-BS
SHEET 2 OF 3
DRAWING NUMBER
REV. B

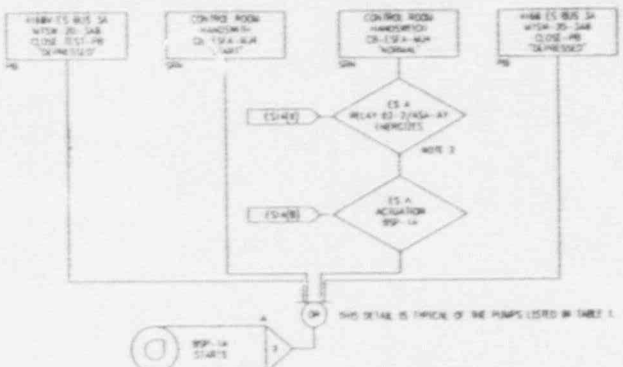


TABLE 1

PUMP	SWITCHGEAR	CONTROL ROOM HANDSWITCH	ES ACTUATION AUTO START SEQUENCE	SPRAY ACTUATION LOGIC	TRANSFER FLAG
BSP-1A	4160V ES BUS 3A SOUTH WTSW-20-3AB	CB-ESFA-4UH	CHANNEL ASA 63/18-AH	RB SPRAY PUMP 1A	ES14(B) ES14(E)
BSP-1B	4160V ES BUS 3B SOUTH WTSW-3F-3B7	CB-ESFB-4UH	CHANNEL ASB 63/18-AH	RB SPRAY PUMP 1B	ES15(W) ES15(C)

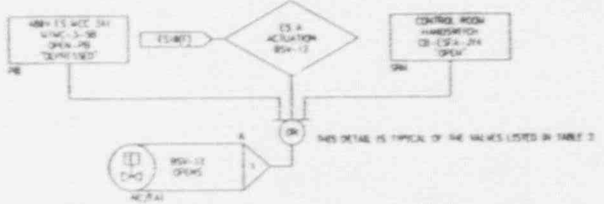


TABLE 2

VALVE	CONTROL ROOM HANDSWITCH	ES ACTUATION	480V ES MCC UNIT	TRANSFER FLAG
BSV-17	CB-ESFA-2H4	ES A	WTMC-3-5B	ES19(E7)
BSV-11	CB-ESFB-2H4	ES B	WTMC-6-3A	ES12(D)

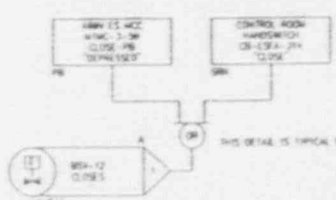


TABLE 3

VALVE	480V ES MCC UNIT	CONTROL ROOM HANDSWITCH
BSV-17	WTMC-3-5B	CB-ESFA-2H4
BSV-11	WTMC-6-3A	CB-ESFB-2H4

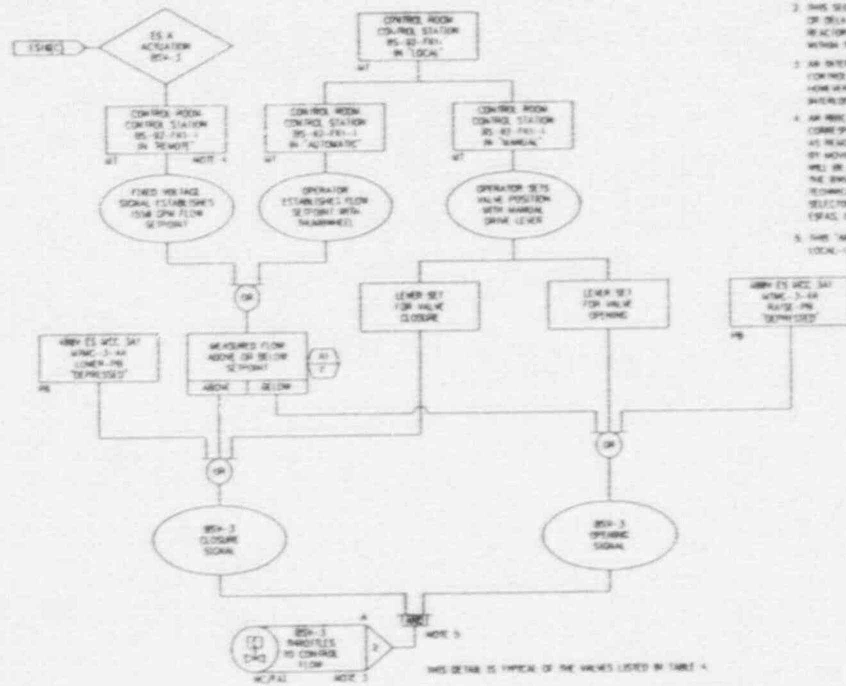


TABLE 4

VALVE	ES ACTUATION	480V ES MCC UNIT	CONTROL STATION	KEY	FLOW TRANSMITTER	TRANSFER FLAG
BSV-3	ES A MBIC BSV-3	WTMC-3-4A	BS-82-FK1-1	A1	BS-WRD-FT1	ES18(E3)
BSV-4	ES B MBIC BSV-4	WTMC-6-3C	BS-82-FK2-1	A2	BS-WRD-FT2	ES13(B3)

NOTES:

1. ALL CONTROL SWITCHES AND TEST SWITCHES ARE ASSUMED TO BE IN THEIR NORMAL / NON-TEST POSITION. ADDITIONALLY, THE REMOTE SHUTDOWN PANEL SWITCHES ARE ASSUMED TO BE ALIGNED SUCH THAT CONTROL IS AVAILABLE FROM THE MAIN CONTROL [illegible]
2. THIS SEQUENCING RELAY CAUSES AUTO-START OF BS PUMP 1A AS EITHER A BLOCK [illegible] OR DELAYED (BLOCK 8) LOAD, DEPENDING UPON THE TIMING OF [illegible] ACTUATION AND HIGH REACTOR BUILDING PRESSURE SIGNALS. THE DETAILS OF THIS LOGIC ARE DEPICTED WITHIN THE ESFAS SFD.
3. AN INTERLOCK [illegible] THE BUILDING SPRAY PUMP SWITCHGEAR AND [illegible] CONTROL VALVE [illegible] ON DRAWINGS [illegible] HOWEVER, THE ELEMENTARY DIAGRAMS FOR THESE VALVES DO NOT REFLECT SUCH AN INTERLOCK.
4. AN MBIC ACTUATION SIGNAL GENERATED BY ESFAS "LOCKS IN" A [illegible] VOLTAGE SIGNAL CORRESPONDING TO A FLOW RATE OF 1550 GPM. THIS MODE OF FLOW CONTROL IS KNOWN AS REMOTE-AUTOMATIC. LOCAL CONTROL MAY BE ESTABLISHED WITHIN THE CONTROL ROOM BY MOVING THE REMOTE-LOCAL SELECTOR LEVER TO THE LOCAL POSITION. THIS ACTION WILL BE REQUIRED TO REDUCE SPRAY FLOW RATE WHEN SWITCHING RB SPRAY SUCTION FROM THE BWST TO THE CONTAINMENT SUMP, DUE TO REDUCED AVAILABLE NPSH. FROM THE TECHNICAL INPUT [illegible], IT WAS NOT CLEAR WHETHER OR NOT THE REMOTE-LOCAL SELECTOR LEVER ON THE FLOW CONTROL STATION OVERRIDES THE MBIC SIGNAL FROM ESFAS, OR WHETHER THIS SIGNAL MUST BE RESET PRIOR TO THROTTLING RB SPRAY FLOW.
5. THIS "AND" GATE INDICATES THAT BOTH REMOTE-AUTOMATIC AND SUBSEQUENTLY EITHER LOCAL-AUTOMATIC OR MANUAL FLOW CONTROL MODES WILL BE REQUIRED.

PRELIMINARY
FOR INFORMATION ONLY
THIS DIAGRAM REFLECTS PLANT CONFIGURATION AS OF AUGUST 8, 1989

NO.	REVISIONS	BY	CHECKED	APPROVED	DATE

FLORIDA POWER CORPORATION
ST. PETERSBURG, FLORIDA
CRYSTAL RIVER PLANT
UNIT NO. 3

SAFETY FUNCTION DIAGRAM
REACTOR BUILDING SPRAY
AND SPRAY ADDITIVE SYSTEM
DETAIL

DRAWN BY JBH DATE 27MAR90
CHECKED BY LWH DATE 27MAR90

IMPELL

APPENDIX F

DESIGN-BASES DOCUMENT ATTRIBUTES

A list and description of fundamental design-bases document attributes determined from documents provided to the survey team and review of other documents prepared by various industry groups is provided below. Utilities that have not begun a design-bases reconstitution program may find this list helpful during the planning phase of their program.

- <u>List of System-Specific Regulatory Requirements and Exceptions</u>

  The regulatory requirements (e.g., general design criteria, <u>Code of Federal Regulations</u>, Title 10, and State, local, and other Federal agencies) applicable to the facility design are defined and any exceptions to the requirements that are reflected in the current plant design are identified.

- <u>List of System-Specific Licensing Commitments and Exceptions</u>

  The applicable industry codes and standards along with a reference to where the commitment was made are identified. Commitments to applicable regulatory guides and programs also are identified. Any exceptions to or interpretations of these requirements that are applicable to the current facility design are provided.

- <u>List of Supporting References</u>

  Reference documentation that supports the parameters, functions, descriptions, design bases, and configuration of the system are identified in sufficient detail to enable retrieval of the document in its current or applicable status from utility document control systems. References that are subject to revision to reflect the current as-built plant condition should not include revision identification. Examples of reference documents are listed below.

  drawings
  calculations
  procurement documents
  correspondence
  plant procedures
  licensing documents
  design change documents

- <u>System Functional Description and Design Bases</u>

  The overall system functional and performance requirements are defined along with the basis for each requirement. The various operating modes of the system are identified and the safety classification of the system (safety related and not safety related) is provided for each operating mode. The physical boundaries and functional relationship to interfacing systems are specified.

- <u>Component Descriptions</u>

  Major system components (i.e., those having important system functions) are identified and described, including applicable codes and standards, classifications, functions under applicable operating modes, and performance requirements and their bases.

- <u>Description of System and Component Testing Requirements</u>

  Test requirements for systems and components to demonstrate their acceptable performance are identified and reference to applicable regulatory or industry codes, standards, or commitments is made. Test restrictions under certain plant operating conditions or unusual configurations required to accomplish acceptable test results also are identified.

- <u>Description of the Functional Requirements for Support Systems</u>

  The functional requirements for interfacing systems in support of the subject system are identified. Interfaces between the system and structures (foundations, walls) are included and requirements defined. Control logic, interlocks and sensors, and instrumentation in other systems that affect system operation also are identified.

- <u>Description of System Instrumentation and Control Requirements</u>

  The requirements for instrumentation and controls to ensure proper function and performance of the system are specified. Requirements may arise from application of industry design practices, engineering judgment, reliability, or other factors in addition to regulatory or code requirements.

During the review of utility design-bases document programs, certain notable attributes were observed by the team that enhanced the preparation of the documents, the correspondence of the documents to source documents or requirements, or the usefulness of the documents to the defined primary users. While most of the attributes were unique to one utility or another, a few were found at several utilities. A list and description of these attributes is provided below.

- <u>Description of System and Component Design Limitations</u>

  System and component functional descriptions were enhanced by describing additional limitations imposed by materials and chemistry considerations, or operational considerations or restrictions.

- <u>Historical Summary of System Modifications and Why They Were Made</u>

  A short summary description was included of each modification made to the system since the plant operating license was received and the reason for the modification.

- <u>Description of How Regulatory and Design Bases Were Met</u>

  The listing of the regulatory and design bases and requirements was elaborated and information provided on how each one was met by the system design.

- List of Open Items

  An attachment to the DBD included a list of open items, such as document conflicts, missing or inadequate documentation, unresolved issues of a plant-specific or generic nature, and discrepancies found during plant walkdowns or verification/validation activities during the development of the DBD. If a categorization or prioritization program to resolve the items was developed, this information was included.

- Description of System and Component Design Parameters and Reasons for Selecting Them

  For each design parameter associated with the overall system and the individual components of the system a basis was stated for selection of the parameters (e.g., regulatory requirement, commitment, or good practice).

- System-Based Function Diagrams for Each System Characteristic

  Composite diagrams (success trees) were developed that show the state (e.g., open, closed, running) of active and passive components necessary to complete specific system functions during various accident response modes (e.g., provide low-pressure injection with the makeup pumps in the piggyback mode, achieve containment isolation on a high-high containment pressure signal). See Appendix E to this report for examples.

- System-Based Logic Trees for Each Operating Mode Showing How Regulatory/ Design Requirements are Met

  Logic trees for each system operating mode were developed that show the flow from top-level general design criteria to the safety function of the system mode to the system parameters for the mode and finally to component parameters for the mode. See Appendix E to this report for examples.

- Design-Bases Documents for Safety-Related Structures

  Design-bases documents were developed for safety-related structures, such as the containment, auxiliary building, intake structure, and control room, that define the requirements and bases for those structures that house key safety-related systems and components.

- Design-Bases Documents for Chapter 15 Analyses

  System and component operating parameters were documented, analysis techniques were addressed, and the gross effect on the analysis if a parameter were to change was identified. Accident scenarios were identified and described along with assumptions made by the NSSS vendor in performing the accident analyses. The parameters and assumptions were validated by comparison to plant data and configuration.

- Operational Conditions Matrix

  A matrix was developed showing the required system and system component operating states and operating conditions for each mode of normal operation and transient, abnormal and accident conditions.

- System-Specific Responses to Plant Transients and Accidents

  The specific response of each system during a plant transient or accident was defined.

- Specification of Design Margins

  The margins available for each system and component parameter were defined and these margins separated into design margins and performance margins.

- System-Specific Response to Postulated Failures During Different Plant Operating Modes

  Failures during different plant operating modes were postulated and the system-specific responses expected during these failures were identified to ensure that the design bases encompassed the system responses identified.

- Reasons for System Specific Alarms and Set Points

  The bases and reasoning behind the specification of system and component set points and alarm settings were provided.

- Calculation Summaries

  Summaries of major system calculations were provided along with the basic assumptions, the relationship to other or previous calculations, and the general conclusions of the calculations.

APPENDIX G

DESIGN-BASES DOCUMENT SCOPE

This is a composite listing of plant systems and generic design topics of the design-bases document efforts at the six utilities surveyed.

SYSTEM/STRUCTURE/TOPIC

Auxiliary/emergency feedwater
4-kV system including emergency diesel generator
Nuclear instrumentation
Component cooling water
Auxiliary saltwater
Equipment seismic qualification
Safety injection
Residual heat removal/decay heat removal
12-kV system
480-V system
120-V instrument ac
125- and 250-Vdc system
Instrument classification
Digital feedwater control
Backup air system
Instrument air system
Plant computer
Containment structure
Auxiliary building
Raceway/structural aspects
Pipe stress analysis
Shutdown cooling
Emergency response facilities
Primary and secondary sampling
Post-accident sampling
Records retention
Regulations, codes, and standards
Personnel protection
Core flood
Circulating water system
Integrated control system
Chemical and volume control
Containment spray
Reactor coolant
Spent fuel cooling
Heavy loads
Flooding
Missiles
High-energy line break
Moderate-energy line break
Compressed air
Fire protection
Feedwater system
Turbine steam supply
Appendix R fire protection program

Gaseous radwaste
Liquid radwaste
Heating, ventilation, and air conditioning
Makeup water
Annunciator, temperature monitor, and site emergency alarm systems
Main generator 25-kV, 250-kV, and 500-kV systems
Electrical separation and isolation
Environmental qualification
Grounding system
Cathodic protection
Solid-state protection system/reactor protection system
Radiation monitoring system
Digital rod position indicating system
Fire penetrations
Fuel handling building
HVAC structural duct and supports
Cranes and fuel handling system
Piping support analysis
Active valves
Site meteorology
Demineralized water system
Accident analysis
Control room habitability
Containment isolation
As low as is reasonably achievable
Nuclear steam supply system
Containment H_2 purge system
Post-accident venting
Fuel handling system
Nuclear fuel system
Condensate system
Extraction and heater drip system
Auxiliary steam system
N_2 and H_2 system
Service cooling water system
Lube oil and purification system
Main turbine system
Oily water separator system
Condensate polishing system
Solid radwaste handling and storage system

Hazardous waste system
Electrical cable termination and raceway
Miscellaneous electrical devices
  (motors, etc.)
Lighting, 120-Vac general use, boric
  acid heat trace and cathodic
  protection systems
Communications, security systems
Seismic monitoring system
Safety parameter display system
Nuclear monitoring system
Simulator
Multisystem interface (panels)
Seismic design
Intake structure
Tornado
Tsunami
Reactor vessel level instrumentation system
Welding

APPENDIX H

SELF-ASSESSMENT QUESTIONS FOR DESIGN-BASES DOCUMENT AND DESIGN CHANGE CONTROL PROGRAMS

The following questions are provided to assist utilities in performing an assessment of their design documentation and configuration management systems to determine the need for a design-basis document program.

- Are the design bases for safety-related systems, structures, and components specified and available for use in the design change control program?

- Are there reportability determination and regeneration prioritization programs for missing or inadequate design documentation?

- Is essential design documentation, such as calculations identified, categorized, and weighed against what should be available?

- Does the drawing control program provide timely revisions to drawings required for operations, maintenance, and design activities?

- Is the licensing commitment tracking system oriented to the plant design so that the current licensing bases of the plant are clearly defined?

- Are the design margins for safety-related systems, structures, and components defined and assessed during plant design changes?

- When a potentially reportable event is dispositioned, are you generally able to access the appropriate analysis and test documents?

- If you were to develop design-bases documents for your facility, would your corporate engineering groups as currently configured be able to play a significant role in the research, development, management, guidance, preparation, review, and validation and verification activities of the program?

- Utilizing the guideline design attributes presented in Appendix A to 10 CFR Part 50, assess the retrievability, control, accessibility, and as-built status of the design documentation.

- If your plant is upgrading design technology, do the engineering organizations have sufficient design-bases information available to perform the upgrade? For example, if analog instrumentation is upgraded to digital instrumentation, is there sufficient documentation regarding the power quality, thermal environment, and electromagnetic environment for the more sensitive digital systems?

- During the design change process, does the staff rely on oral historical information provided by senior staff, vendor personnel, or A/E personnel rather than on controlled design documents?

- Is the FSAR used as a design-bases document rather than more detailed information?

- How useful and accurate are the system descriptions for the plant? Do they adequately describe the bases for design decisions in addition to describing the design configuration?

The following questions are provided to assist utilities in performing an assessment of their design control programs to determine the need for changes or enhancements.

- Do your corporate and plant engineering groups maintain a comprehensive set of design specifications, guidelines, and standards for the design change process? Assess the coverage these documents provide for the design attributes presented in Appendix A to 10 CFR Part 50.

- Do you prepare most significant design modifications to your plant as opposed to relying on the original plant architect-engineer and other contracting organizations?

- If you contract most significant design modifications to the original plant architect-engineer and other contracting organizations, do you require them to prepare them to your own design specifications and standards as opposed to relying on their individual specifications and standards?

- If you contract most design modifications to the original plant architect-engineer and other contracting organizations, do you perform engineering assurance checks of the design modification packages these organizations prepare?

- Do you maintain your own files of design documents, drawings and calculations, as opposed to letting the original plant architect-engineer and other contracting organizations maintain them?

- Do you maintain in-house computer programs to perform structural analysis and piping analysis?

- Does the technical competency within your corporate and plant engineering groups reside with employee rather than contracted engineers?

- Do you maintain as-built flow diagrams and piping physicals drawings for all safety-related piping systems for your plant?

- Does your drawing program provide revised, as-built drawings to the control room files at modification turnover?

- Does your design change control program adequately identify and control incremental changes to design calculations?

- Is supporting documentation for past plant modifications (e.g., calculations and analyses, and safety evaluations) available and adequate?

- Do you have a formal program for turnover of modifications to operations?

- When preparing design modifications, do engineering personnel use a comprehensive checklist of design attributes as a tool for making design decisions? How are the design attributes, such as those addressed in Appendix A to 10 CFR Part 50, addressed during the modification process?

- Do you maintain as-built control logic diagrams for other than instrumentation and control personnel to determine interlock and control requirements?

- Do you maintain as-built instrument loop diagrams?

- Have you assigned systems engineer responsibilities in both the plant and the corporate design engineering organizations?

APPENDIX I

TYPICAL DESIGN ATTRIBUTES AND CONTROLLING DESIGN PARAMETERS TO FORM THE BASIS OF A TEMPLATE

The following is a list of typical design attributes and controlling design parameters that could form the basis for a template:

Electrical

- Diesel generator sizing
- Safety-related power cable sizing
- Safety-related system voltage profile
- Safety-related system short circuit analysis
- Diesel generator performance
- Safety-related bus transfer analysis
- 480-V MCC and switchgear protection and coordination
- Class 1E battery sizing
- Uninterruptable power supply sizing
- Low voltage and dc cable sizing
- Class 1E ac/dc system protection and coordination
- Safety-related instrument set point, and accuracy calculations
- Control loop response time calculations
- Electrical separation analysis
- Raceway fill and loading

Nuclear

- Control room toxic gas
- Tornado loadings and external missiles
- External flooding effects
- Pipe break effects (i.e., pressure, temperature, flooding, rupture)
- Equipment environmental qualification (harsh and mild environment)
- Systems required to mitigate design-bases accidents (DBAs)
- Radiation source terms for DBAs
- Containment analytical model
- Post-accident conditions
- Offsite dose analysis for normal operation and DBAs
- Control room shielding and operator doses
- Personnel radiation doses during DBA recovery activities
- Airborne radioactivity transport from a fuel handling DBA
- Loss of spent fuel pool cooling
- Ultimate heat sink capacity analysis
- Control room habitability during blackout (air temperature)
- Anticipated transient without scram events
- Pipe break discharge flow
- Secondary containment air pressure control analysis
- Heat load determination analysis
- Heating, ventilation, and air conditioning (HVAC) system failure modes and effects analysis
- HVAC instrumentation set points
- Control room enclosure air infiltration
- Battery compartment hydrogen accumulation
- HVAC design analysis
- Reactor transient analytical models

Reactor coolant system transient analysis
Pipe flow hydrodynamic loads analysis
Piping network dynamic flow analysis
Valve operability analysis
ASME Code of record calculations
Computer code certification documents
Thermal analysis of components, supports, and structures
Component minimum wall thickness calculations

Civil

Category I reinforced concrete structures analysis
Category I steel structures analysis
Civil structure dynamic/earthquake analysis
Dynamic/stress analysis of substructures
Dynamic/stress analysis of containment, nozzles, etc.
Tornado analysis of structures
Category I weld evaluations
Category I structure block walls
Component seismic/structural qualification
Pipe rupture restraints
Bolt anchorage in Category I structures
Probable maximum flood analysis
Platform steel, cranes, monorails, doors, ladders
Heavy loads analysis
Category I piping analysis
Seismic analysis of electrical conduit
Instrument line analysis
Category I supports analysis (pipe, duct, conduit, tray and instrumentation, and NSSS supports)
Penetration qualification
Earthquake ground motions
Category I foundation analysis

Mechanical

Piping minimum wall thickness
Pump net positive suction
Pump total system head
Valve pressure drops (Cv)
Tank nozzle/branch line reinforcement
Heat transfer (sizing Hx, condensers, heaters etc.)
Pump/system performance
Pressure/vacuum relief valve sizing
Sump capacity
Cooling water flow rates
Equipment performance calculations
Corrosion/erosion allowances
Tanks (volume, wall thickness, etc.)
Pipe sizing/flow
System design/operating pressures and temperatures
Pump brake-horsepower requirements
Valve actuation times and check valve closure

APPENDIX J

TYPICAL CATEGORIZATION OF DESIGN DOCUMENTS BY ORDER OF SAFETY SIGNIFICANCE

Use of a prioritization methodology in considering whether to regenerate missing or deficient documents can ensure that the licensee focuses resources on the more safety-significant items in a timely manner. An initial screening process would enable the licensee to determine the significance, effect on plant operability, and reportability requirements related to the missing or inadequate documentation.

One way the survey team used to rank the importance of design documents according to safety significance is given below.

Category 1 - Design documentation that supports or defines technical specification safety limits, limiting conditions for operation, limiting safety system set points or surveillance requirements. These documents demonstrate that the systems, structures, and components (SSC) addressed by technical specifications will perform their active safety functions.

Category 2 - Design documentation that defines controlling parameters or demonstrates the active functionality of safety-related SSC that are not explicitly addressed by the technical specifications, but that support the SSC addressed by technical specifications, such as heating, ventilating, and air conditioning systems.

Category 3 - Design documentation that defines controlling parameters or demonstrates active functionality of safety-related SSC not included in categories 1 or 2 above.

Category 4 - Design documentation that defines controlling parameters or demonstrates the functionality of safety-related SSC with regard to passive considerations (e.g., seismic considerations).

Category 5 - Design documentation that demonstrates the design of non-safety SSC is such that its failure would not impair the functionality of safety-related SSC (e.g., seismic considerations related to seismic classification Categories I and II).