Docket Nos.: 50-445
and 50-446

AUG 13 1985

APPLICANT: Texas Utilities Electric Company

FACILITY: Comanche Peak Steam Electric Station, Units 1 and 2

SUBJECT: SUMMARY OF THE STAFF'S AUDIT OF THE COMANCHE PEAK SAFETY PARAMETER DISPLAY SYSTEM (SPDS)

On June 25 and 26, 1985, the staff performed an audit of the Comanche Peak SPDS. The purpose of audit was to review outstanding questions regarding the Verification and Validation (V&V) programs, to confirm that the V&V program is being correctly implemented, to audit the V&V results to date, and to audit the installed SPDS at Unit 1.

The enclosed summary describes significant events in the audit, contains copies of the Vu-graphs that were presented to the staff, and lists the attendees. The staff observations, notes and conclusions presented in the exit briefing are listed.

S. B. Burwell, Project Manager
Licensing Branch No. 1
Division of Licensing

Enclosure: As stated

cc: See next page

LB#1/DL	LB#1/DL	CP/TRT/DL	CP/TRT/DL
SBurwell/mac	BJYoungblood	CIhammell	VSNoonan
08/12/85	08/12/85	08/12/85	08/13/85

SUMMARY OF THE STAFF'S AUDIT

OF THE COMANCHE PEAK SPDS,

June 25 - 26, 1985

On June 25 and 26, 1985 the staff performed an audit of the Comanche Peak SPDS. The purpose of the meeting was to attempt to resolve outstanding questions regarding the Verification and Validation (V&V) program, to confirm that the V&V program is being correctly implemented, to audit the V&V results to date, and to audit the installed SPDS at Unit 1.

The NRC team leader, George Lapinsky of the Human Factors Engineering Branch, was assisted in the audit by consultants from Lawrence Livermore National Laboratory and Comex. A list of attendees is included here as Enclosure 1.

On June 25, 1985 representatives of the Texas Utilities Generating Company (TUGCo) presented information regarding the Comanche Peak SPDS design and implementation. Copies of Vu-graphs used during the presentations are included here as Enclosure 2. In addition, the audit team examined the following reports:

1. "Functional Design Specification for SAS Software," Rev. 2, May 20, 1982; by Quadrex for Ad Hoc Committee on Instrumentation Systems, SAS Project.

2. "Industrial Design/Human Factors Guidelines and Abbreviations", SASLOG-33, May 15, 1981; by Quadrex.

3. "Safety Assessment System Evaluation Program Report," SASLOG-105, May 20, 1982; by Quadrex and Inpsych Company.

4. "Training Manual for Initial On-Site Safety Assessment System (SAS) Training Program," by Quadrex.

5. "Project Plan for SAS/ERF Computer System for Comanche Peak Unit #1," by Quadrex, for Texas Utilities Services, Inc., CPSES.

6. "System Functional Specification, CPSES Unit 1, SAS/ERF Computer System," December 8, 1981; by Quadrex, for Texas Utilities Services, Inc.

7. "System Software Design Specification," QUAD-2-82-003, three volumes, Rev. 3 April 3, 1984; by Quadrex, for Texas Utilities.

8. "System Hardware Design Specification," QUAD-2-82-004, Rev. 2, May 18, 1984; by Quadrex, for Texas Utilities.

9. "Verification and Validation Plan for the SAS/ERF Computer System for Texas Utilities Comanche Peak Unit 1," October 1983, by the Boeing Company.

10. "System Requirements Review Report, CPSES Unit 1, SAS/ERF Computer System," Document No. D275-50010-1, November 1981, by The Boeing Company.

11. "Verification and Validation Report, SAS ERF Computer System, CPSES Unit 1," August 31, 1984; by The Boeing Company.

12. "Phase 1-1/2 Verification and Validation Report, Safety Parameter Display System for The Texas Utilities CPSES Unit 1," QUAD-4-85-014 Draft, April 30, 1985; by Quadrex, for Texas Utilities Company.

There were also Test Plans and Test Reports available from the V&V report series. The conduct and results of the tests are summarized in the Verification and Validation Report. Also available was a series of letters from the SPDS design contractor, Quadrex, to Texas Utilities documenting SPDS design additions and plant-specific changes requested by the utility, the design team's review, and final design of the changes.

On June 26, 1985 the staff toured the Unit 1 control room and witnessed a demonstration of the SPDS functions at the Technical Support Center computer console. Afterwards an audit of the display page formats was done. The audit concluded in an exit briefing, at which time the staff presented the following observations, notes, and conclusions:

1) It appears that no final review and dynamic testing was done on the installed system - the staff feels this is necessary since the system has been revised since the original testing that was done on the generic vendor prototype.

2) No final conclusion can be drawn regarding the choice of SPDS parameters until the Procedures and Systems Review Branch (PSRB) completes its review. However, it appears that Main Stack Radiation Level and/or Release Rate are missing from the SPDS.

3) The Instrumentation and Control Systems Branch (ICSB) has reviewed and approved, on an interim basis, the isolation devices used on the SPDS. The audit team saw nothing that would contradict the ICSB conclusions.

4) The data validation methodology for single input parameters is weak and is acceptable only as an interim solution.

5) Human factors were considered in the design and the SPDS reflected good human engineering practices except for two items: a) severe glare on the display screen, and b) overprinting of trend graphs, one upon the other, to the point of unreadability.

6) Reliability/availability appears to be built into the system through redundancy. However, estimates and/or empirical data do not exist to confirm that the system will be highly reliable and available.

ENCLOSURE 1

June 25, 1985

Attendance List

Name	Organization
Don Woodlan	TUGCO - Licensing
Mark A. Coffing	TUGCO Nuclear Engineering
John T. Grillo	TUGCO Nuclear Engineering
Bob Hagan	TUGCO Nuclear Engineering
Ron Estes	QUADREX
Dennis R. Johnson	QUADREX
Russell Smith	TUGCO - Operations Support
Norman Terrel	TUGCO - Operations Support
Bill O'Connell	Lawrence Livermore National Lab
George Lapinsky	NRC - Human Factors Engineering
Gary W. Bethke	NRC - COMEX
Tom J. Talley	TUGCO

June 26, 1985

Name	Organization
Bob Hagan	TUGCO Nuclear Engineering
Mark A. Coffing	TUGCO Nuclear Engineering
Tom J. Talley	TUGCO Advanced Systems Engineering
J. T. Grillo	TUGCO Nuclear Engineering
W. R. Woodlan	TUGCO Licensing
R. D. Calden	TUGCO Nuclear Engineering
D. R. Johnson	Quadrex
Ron Estes	Quadrex
Norman Terrel	TUGCO Operations
Bill O'Connell	Lawrence Livermore National Lab
Gary Bethke	NRC - COMEX
George Lapinsky	NRC- HFEB

ENCLOSURE 2

OVERVIEW OF THE PROJECT WHICH DEVELOPED THE COMANCHE PEAK STEAM ELECTRIC STATION SAFETY PARAMETER DISPLAY SYSTEM

Presented to
the NRC Audit Team
June 25, 1985

by
Dr. Tom Talley
Texas Utilities Generating Company

TMI

NRC
WESTINGHOUSE OWNERS
EPRI/NSAC

THE SAS GROUP

THE CPSES SITE-SPECIFIC
IMPLEMENTATION

SPDS
CSFM
ERF

WESTINGHOUSE OWNERS GROUP (W.O.G.)

AD HOC COMMITTEE ON INSTRUMENTATION --

COMMITTEE MEMBERS PROVIDED

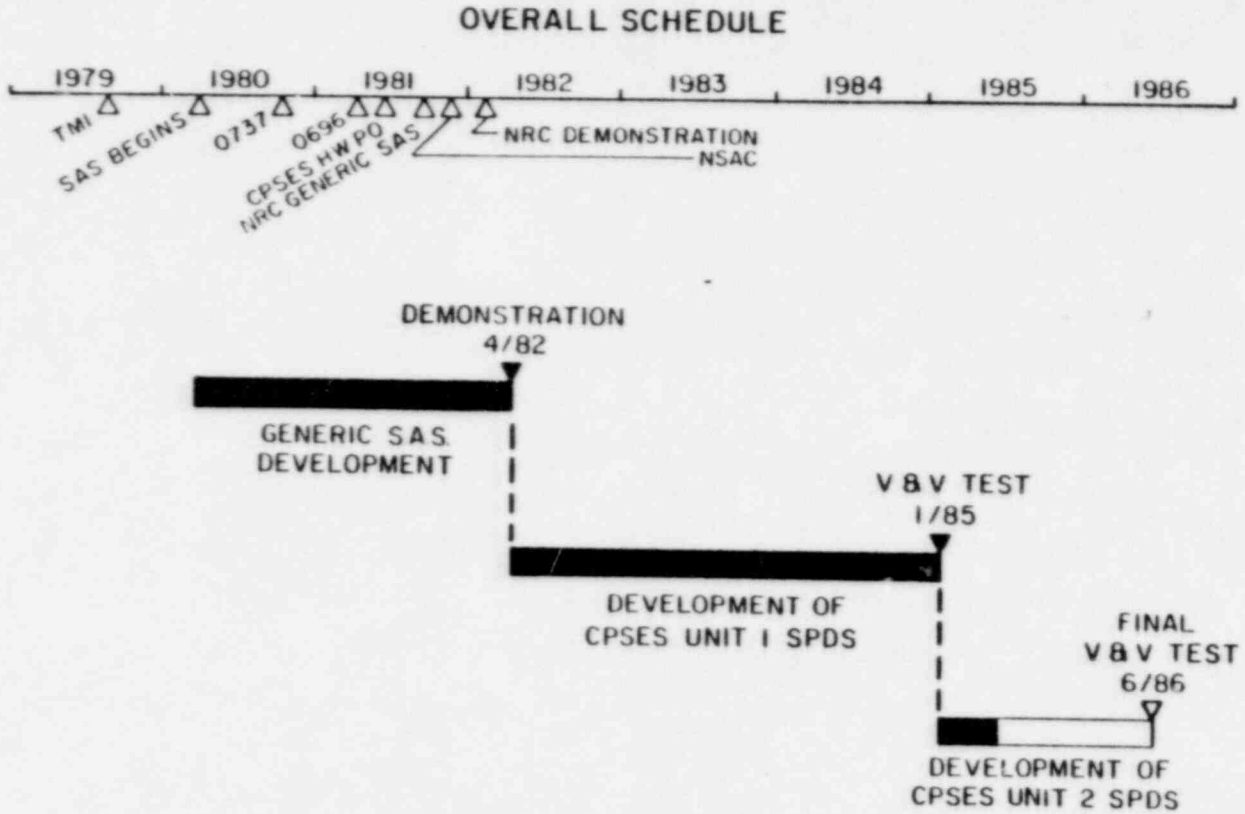
A BROAD RANGE OF EXPERIENCE TO

PRODUCE THE SAFETY ASSESSMENT SYSTEM.

S.A.S. COMMITTEE MEMBER UTILITIES --

FLORIDA POWER & LIGHT
WISCONSIN ELECTRIC
WISCONSIN PUBLIC SERVICE
ROCHESTER GAS & ELECTRIC
COMMONWEALTH EDISON
CONSOLIDATED EDISON
PUBLIC SERVICE OF INDIANA
NORTHERN STATES POWER
SNUPPS
TAIWAN POWER
SWEDISH STATE POWER BOARD
TEXAS UTILITIES GENERATING CO.

THE CPSES ERF COMPUTER SYSTEM IS A SITE-SPECIFIC IMPLEMENTATION OF APPROPRIATE PARTS OF THE GENERIC SAFETY ASSESSMENT SYSTEM DEVELOPED BY THE W.O.G. AD HOC COMMITTEE ON INSTRUMENTATION SYSTEMS



THE W.O.G. AD HOC COMMITTEE
THAT DEVELOPED THE GENERIC S.A.S.
INCLUDED SEVERAL SUBCOMMITTEES --

HARDWARE -- SELECTED CPU & DISPLAY HARDWARE

SOFTWARE -- DEVELOPED SOFTWARE DESIGN

SIMULATOR -- DEVELOPED SIMULATOR TEST PROGRAM

VERIF & VALID -- AUDITED DESIGN &
DEVELOPMENT EFFORTS

THE VERIFICATION & VALIDATION SUBCOMMITTEE
VALIDATED THE GENERIC S.A.S. --

V & V FUNCTIONS

-- OVERSEE & REVIEW VENDOR V&V EFFORTS

-- CONDUCT DESIGN REVIEWS

-- REVIEW & APPROVE VENDOR TESTS & RESULTS

-- AUDIT ENGINEERING TEST & CODE WALKTHROUGHS

-- WITNESS SYSTEM TESTS

PROOF OF CONCEPT AND
DESIGN VALIDATION TESTS
OF THE GENERIC S.A.S.
WERE CONDUCTED ON A PWR SIMULATOR--

PHASE 1 - CAPTURE TRANSIENTS
- REPRESENTATIVE SAMPLE
OF NSAC 40 EVENTS
- ROD EJECTION
- 1% LOCA
- SGTR

PHASE 2 - ENGINEERING EVALUATION AT SIMULATOR
- 19 TRANSIENTS

PHASE 3 - OPERATOR EVALUATION
- 6 SCENARIOS
INCLUDING EPRI/NSAC 40
DRAFT GUIDANCE
- 4 CREWS
- WITH & WITHOUT S.A.S.
- FULL DEBRIEFING AFTER EACH

- EVALUATION PROGRAM REPORT

- EPRI RETAINS TRANSIENT TAPES FOR FUTURE USE

THE S.A.S. DOCUMENTATION PACKAGES

AVAILABLE FOR REVIEW INCLUDE --

R.F.Q. FROM AD HOC COMMITTEE

FUNCTIONAL DESIGN SPECS VOL I & II

HARDWARE EVALUATION REPORT

TRAINING PROGRAM

EVALUATION PROGRAM REPORT

VERIFICATION & VALIDATION REPORT

S.A.S. LOG W/ RESUMES OF PERSONNEL

PRESENTATION GRAPHICS FOR
NOV 1981 NRC BRIEFING

PRESENTATION GRAPHICS FOR
APR 1982 NRC DEMONSTRATION

SITE-SPECIFIC IMPLEMENTATION
OF THE CPSES E.R.F. COMPUTER SYSTEM
BEGAN WITH A FULLY VALIDATED SYSTEM --

-- S.A.S. WAS DEVELOPED UNDER
A FULLY DOCUMENTED V&V PROGRAM

-- THE S.A.S. PROJECT INCLUDED
EXTENSIVE EVALUATION TESTS
AT THE INDIAN POINT SIMULATOR
WHICH VALIDATED THE
GENERIC S.A.S. SYSTEM

CPSES SITE SPECIFIC

ERF COMPUTER

IMPLEMENTATION

INCLUDING

SAFETY PARAMETER DISPLAY SYSTEM

ANY COMPUTER-BASED

INFORMATION SYSTEM

INCLUDES THREE BASIC PROCESSES --

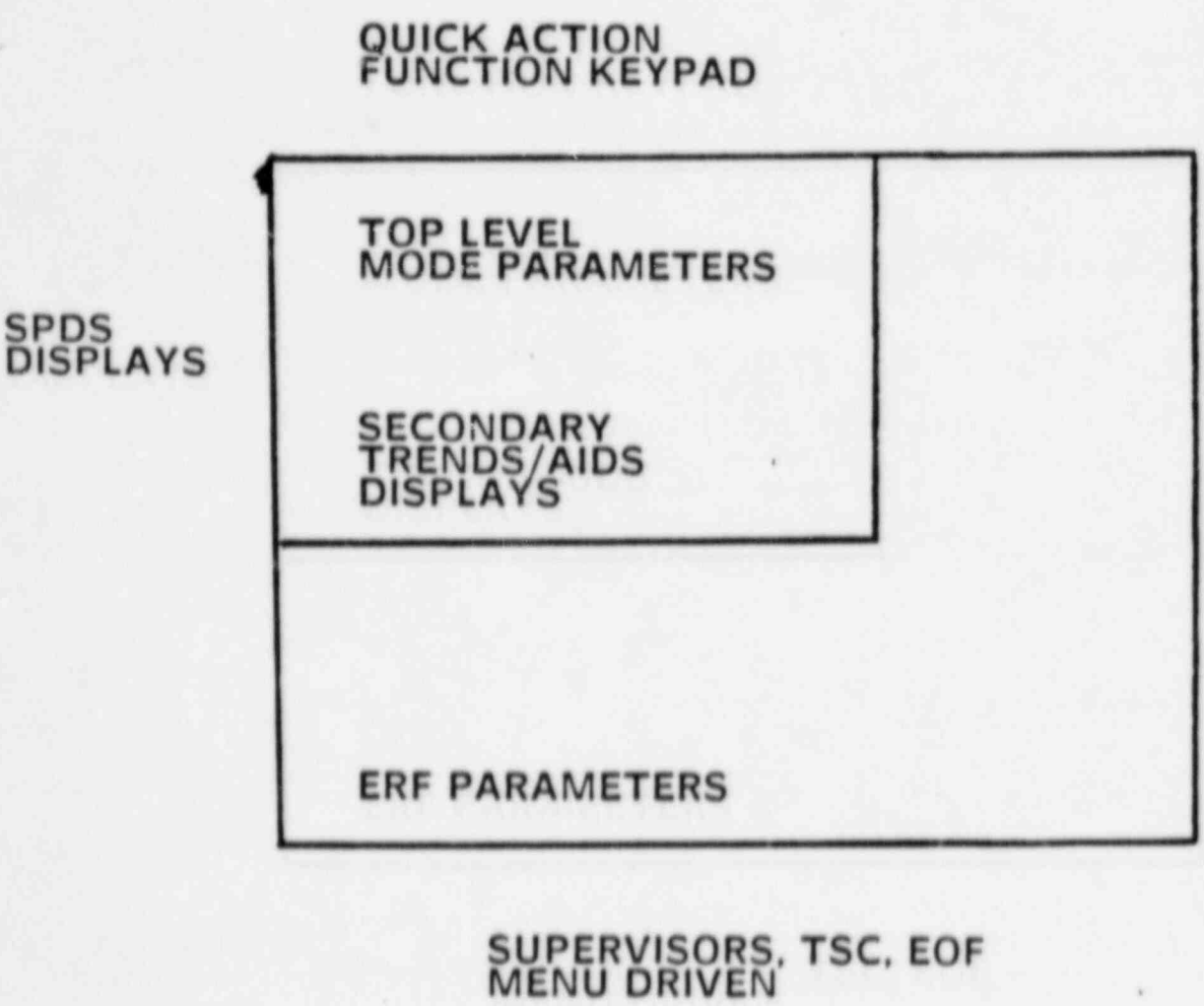
DATA
AQUISITION

DATA
PROCESSING
& STORAGE

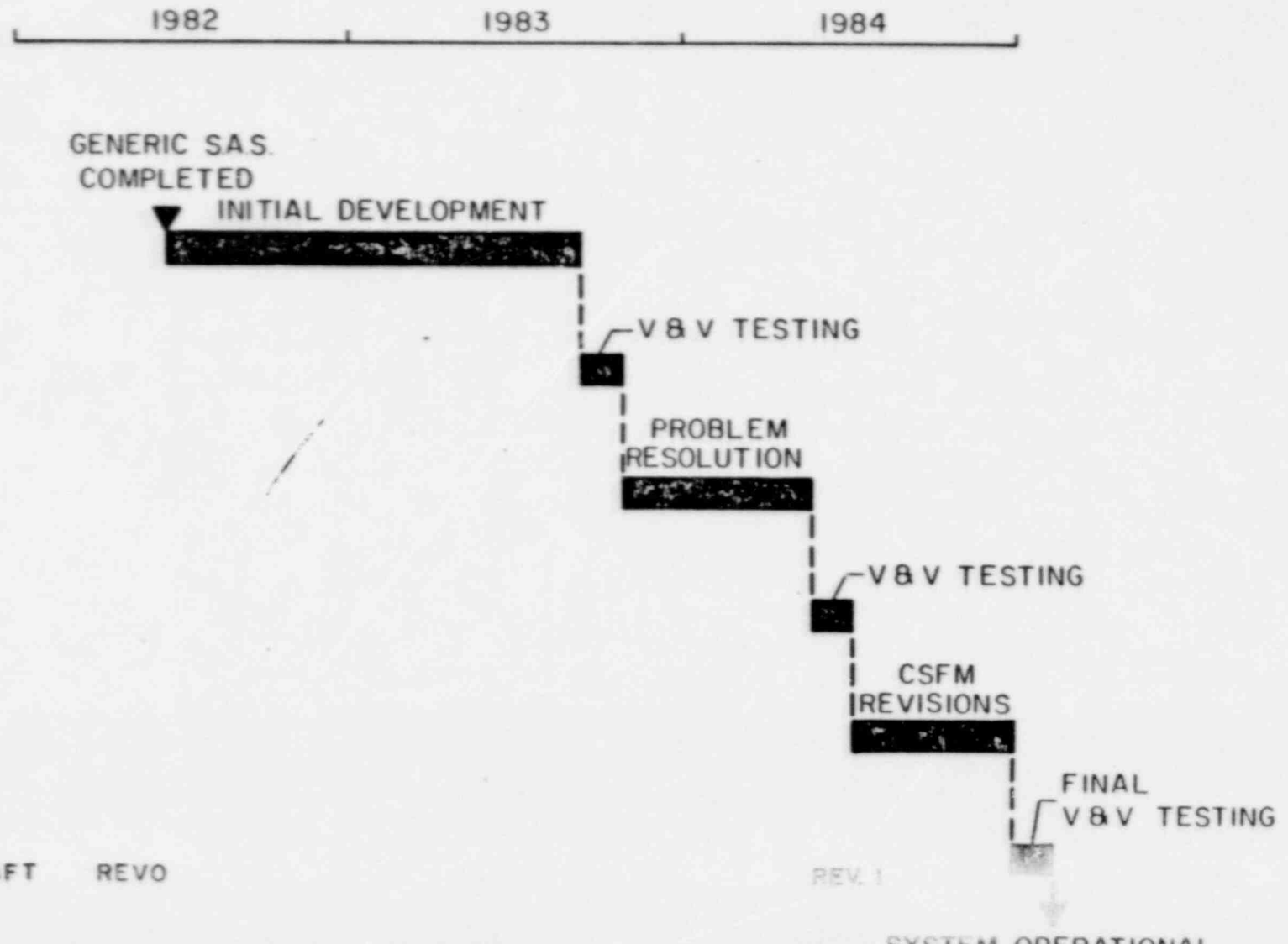
DATA
DISPLAY

THE S.P.D.S. DISPLAYS ARE A SUBSET OF

THE ERF COMPUTER SYSTEM DATA BASE --



IMPLEMENTATION OF THE UNIT 1 ERF COMPUTER SYSTEM INCLUDED THREE MAJOR PHASES



DEVELOPMENT OF THE
UNIT #2 ERF COMPUTER SYSTEM
IS SCHEDULED TO BE COMPLETE IN JUNE 1986 --

- INCLUDES ADDITIONAL PARAMETER INPUTS & ASSOCIATED DISPLAYS

  - INPUT FROM THE REACTOR VESSEL LEVEL INDICATION SYSTEM

- INCLUDES ADDITIONAL NON-SPDS DISPLAYS AND FEATURES

  - METEOROLOGICAL DATA ENHANCEMENT
  - AREA RADIATION MONITOR DISPLAYS
  - CORE EXIT TEMPERATURE DISPLAY
  - HISTORY PLOT FUNCTION
  - OTHER DISPLAYS TO ENHANCE ACCESS TO DATA

OUTLINE OF REMAINING PRESENTATIONS

I. PARAMETER SET SELECTION

- SPDS
- ERF

II. ACCURATE, RELIABLE PROCESSING

- DATA AQUISITION
- COMPUTER SYSTEM
- DISPLAY SYSTEM

III. HUMAN-FACTORED DISPLAYS

- QUICK SPDS
- MENU-DRIVEN DETAIL

SUMMARY OF
PROJECT ORIGIN & STATUS

------***------

- THE CPSES ERF COMPUTER SYSTEM
  IS BASED ON THE GENERIC S.A.S.

- THE SPDS IS AN INTEGRAL PART
  OF THE ERF COMPUTER SYSTEM

- THE UNIT #1 SYSTEM IS OPERATIONAL

- THE UNIT #2 SYSTEM IS UNDER DEVELOPMENT

THE PARAMETER SET

FOR THE

ERF COMPUTER SYSTEM

HAS BEEN VALIDATED

PRESENTED TO THE

NRC AUDIT TEAM

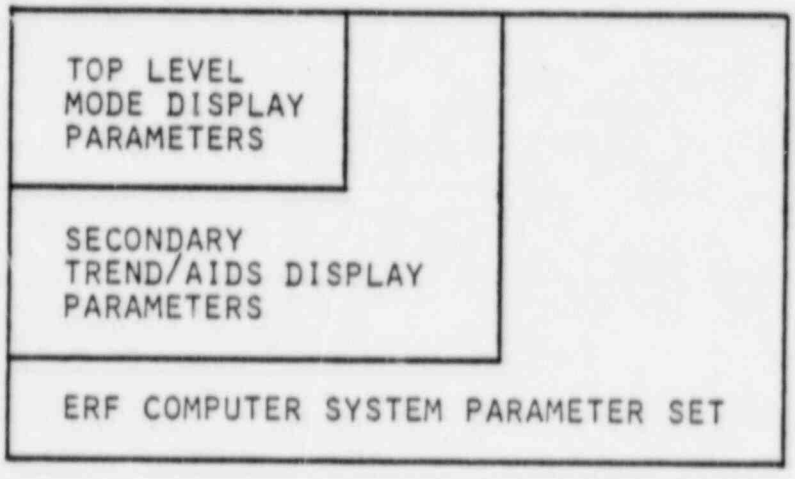
JUNE 25, 1985

BY

BOB HAGAR

TUGCO NUCLEAR ENGINEERING

THE ERF COMPUTER SYSTEM PARAMETER SET INCLUDES TWO IMPORTANT SUBSETS



THE GENERIC S.A.S. SPDS PARAMETER SET IS MONITORED THROUGH THE TOP LEVEL DISPLAY

PARAMETER	S.A.S. SPDS	TOP-LEVEL DISPLAY
REACTOR COOLANT SYSTEM PRESSURE	X	X
PRESSURIZER LEVEL	X	X
REACTOR VESSEL LEVEL	X	X
STEAM GENERATOR PRESSURE	X	X
STEAM GENERATOR LEVEL	X	X
CORE EXIT TEMPERATURE	X	X
MARGIN OF SUBCOOLING	X	X
LOOP COLD-LEG TEMPERATURES	X	X
CONTAINMENT RADIATION	X	X
CONTAINMENT PRESSURE	X	X
CONTAINMENT WATER LEVEL	X	X
POWER-RANGE NUCLEAR POWER	X	X
INTERMEDIATE-RANGE NUCLEAR POWER	X	X

THIS PARAMETER SET WAS VALIDATED DURING THE GENERIC S.A.S. PROGRAM

- PARAMETERS WERE SELECTED BY EXPERIENCED PERSONNEL AFTER CONSIDERING INDUSTRY RECOMMENDATIONS

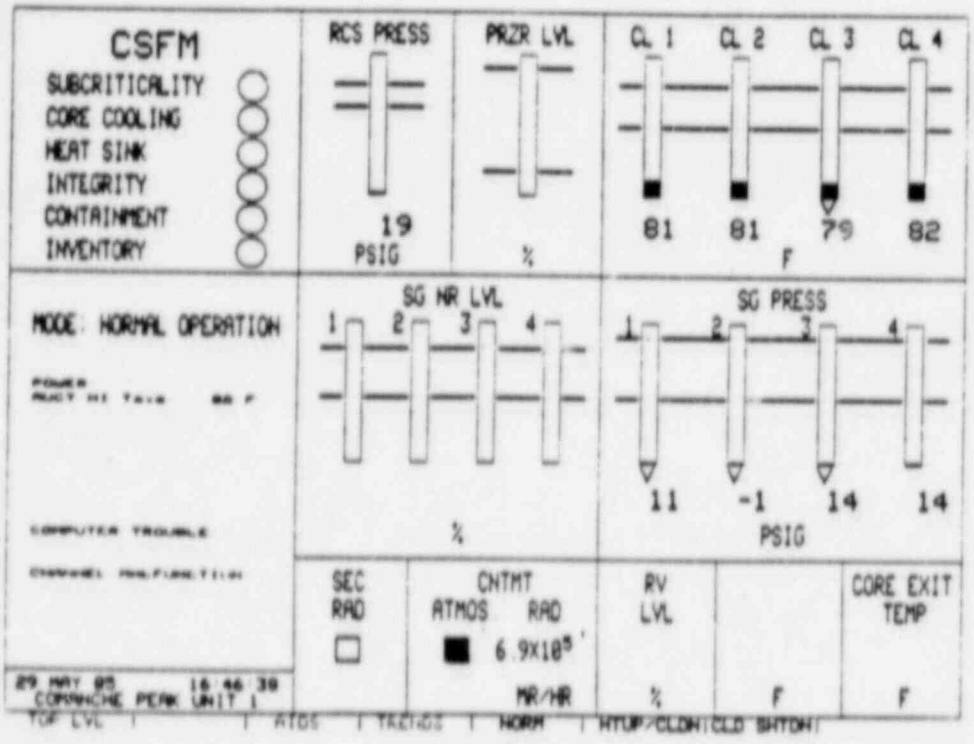
  - AN SPDS MINIMUM PARAMETER SET WAS RECOMMENDED BY THE ATOMIC INDUSTRIAL FORUM

  - AN SPDS PARAMETER SET WAS RECOMMENDED IN NSAC-8

- THE PARAMETER SET WAS EVALUATED BY ENGINEERING PERSONNEL AND CONTROL ROOM OPERATORS DURING THE GENERIC S.A.S. PROGRAM

- EVALUATIONS CONCLUDED THAT THE PARAMETER SET WAS SUFFICIENT TO ALLOW THE OPERATOR TO ASSESS THE OVERALL SAFETY STATUS OF THE PLANT

THESE PARAMETERS ARE PRESENTED ON THE TOP LEVEL DISPLAY



THE CPSES EMERGENCY RESPONSE GUIDELINE PROCEDURES MONITOR SIX CRITICAL SAFETY FUNCTIONS

CRITICAL SAFETY FUNCTIONS

SUBCRITICALITY

CORE COOLING

HEAT SINK

INTEGRITY

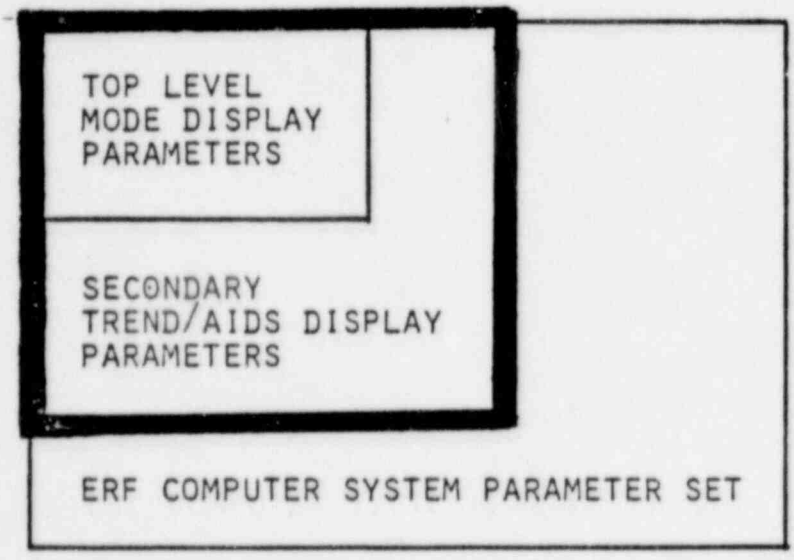
CONTAINMENT

INVENTORY

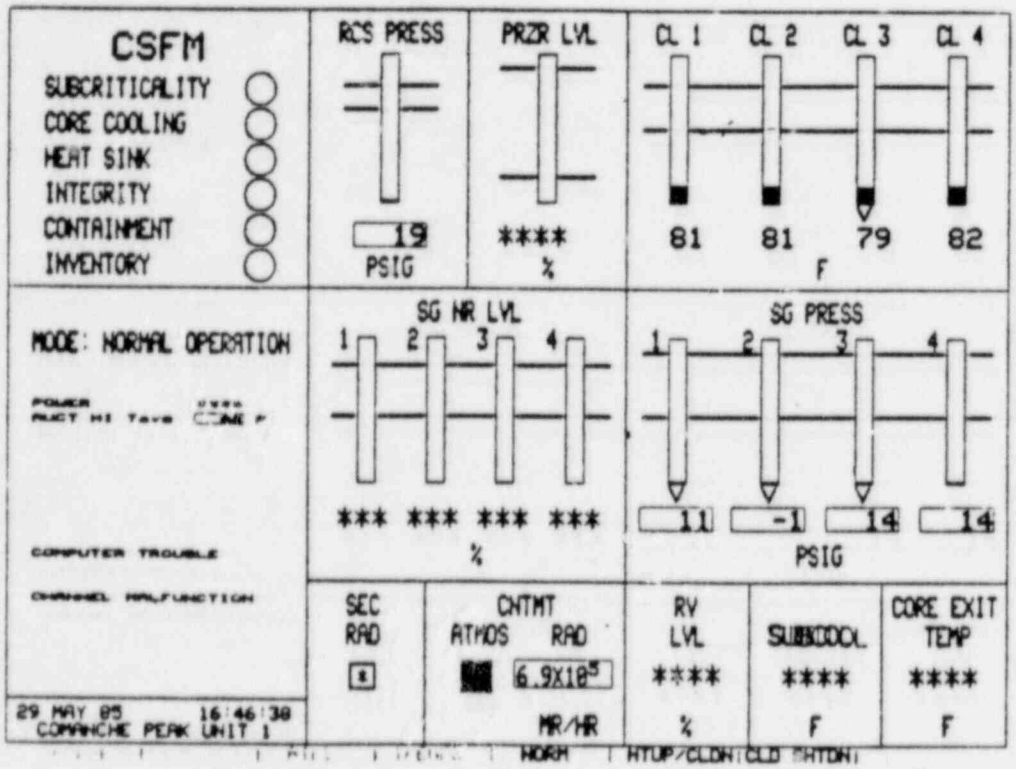
THESE CRITICAL SAFETY FUNCTIONS ARE DEFINED IN TERMS OF A PARAMETER SET

PARAMETER	SUBCRITICALITY	CORE COOLING	HEAT SINK	INTEGRITY	CONTAINMENT	INVENTORY
POWER-RANGE NUCLEAR POWER	X					
INTERMEDICATE-RANGE NUCLEAR POWER	X					
SOURCE-RANGE NUCLEAR POWER	X					
CORE EXIT TEMPERATURE		X				
MARGIN OF SUBCOOLING		X				
STEAM GENERATOR LEVEL			X			
STEAM GENERATOR PRESSURE			X			
AUXILIARY FEEDWATER FLOW			X			
COLD-LEG LOOP TEMPERATURE				X		X
HOT-LEG LOOP TEMPERATURE				X		X
PRESSURIZER PRESSURE				X		
CONTAINMENT PRESSURE					X	
CONTAINMENT WATER LEVEL					X	
CONTAINMENT RADIATION					X	
PRESSURIZER LEVEL						X
REACTOR VESSEL LEVEL						X

THE TRENDS/AIDS DISPLAY PARAMETER SUBSET INCLUDES ALL OF THE PARAMETERS NECESSARY TO MONITOR THESE CRITICAL SAFETY FUNCTIONS



A SUMMARY OF THE STATUS OF THESE CRITICAL SAFETY FUNCTIONS IS INCLUDED ON SPDS DISPLAYS



NUREG-0737, SUPPLEMENT 1 IDENTIFIED FIVE CRITICAL SAFETY FUNCTIONS

CRITICAL SAFETY FUNCTIONS

REACTIVITY CONTROL

REACTOR CORE COOLING AND
HEAT REMOVAL FROM THE PRIMARY SYSTEM

REACTOR COOLANT SYSTEM INTEGRITY

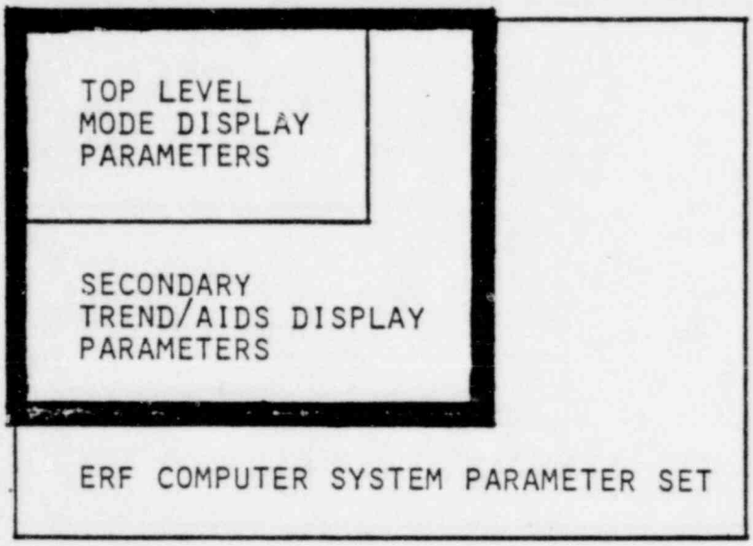
CONTAINMENT CONDITIONS

RADIOACTIVITY CONTROL

THESE CRITICAL SAFETY FUNCTIONS ARE DEFINED IN TERMS OF A PARAMETER SET

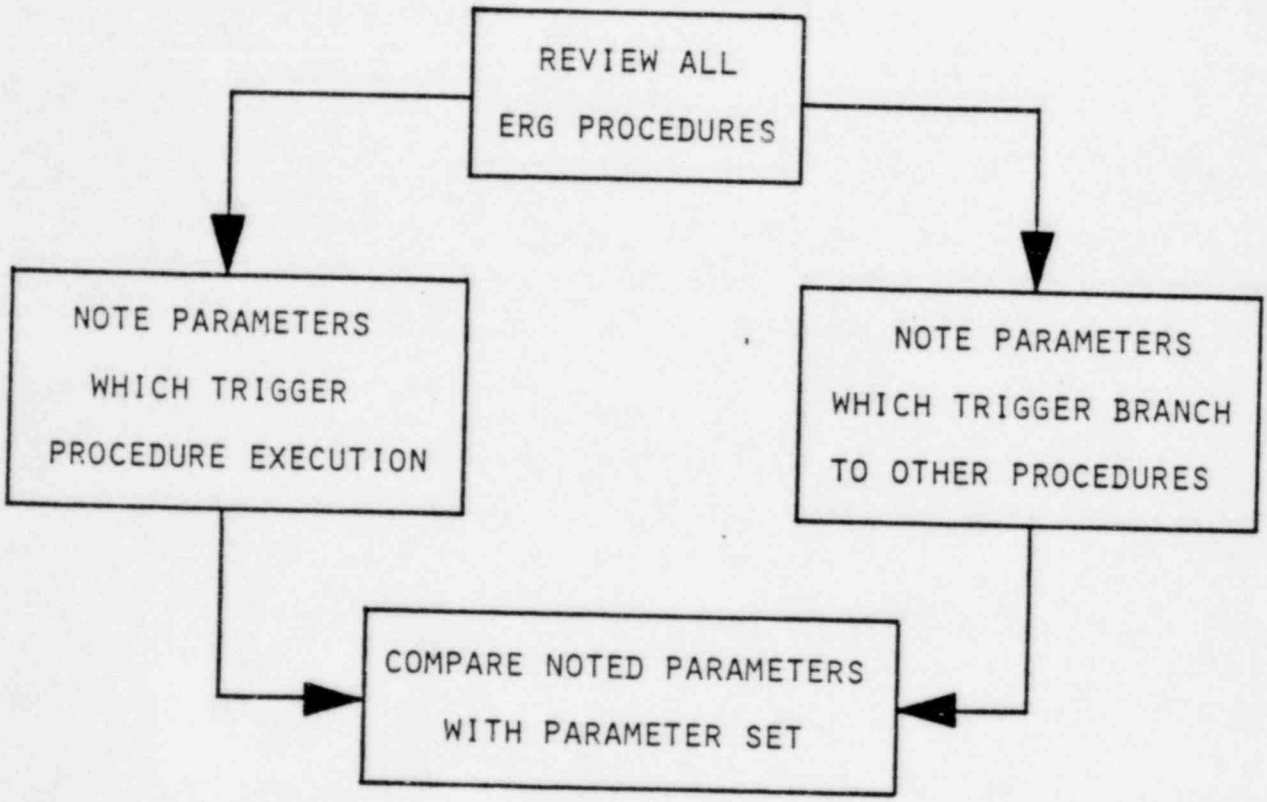
PARAMETER	REACTIVITY	CORE COOLING/HEAT REMOVAL	INTEGRITY	CONTAINMENT	RADIOACTIVITY
POWER-RANGE NUCLEAR POWER	X				
INTERMEDIATE-RANGE NUCLEAR POWER	X				
SOURCE-RANGE NUCLEAR POWER	X				
REACTOR VESSEL LEVEL		X	X		
PRESSURIZER LEVEL		X	X		
CORE EXIT TEMPERATURE		X			
HOT-LEG LOOP TEMPERATURE		X	X		
COLD-LEG LOOP TEMPERATURE		X	X		
PRESSURIZER PRESSURE		X	X		
STEAM GENERATOR LEVEL		X			
STEAM GENERATOR PRESSURE		X			
AUXILIARY FEEDWATER FLOW		X			
STEAM GENERATOR STEAM FLOW		X			
CONTAINMENT TEMPERATURE				X	
CONTAINMENT PRESSURE			X	X	
CONTAINMENT WATER LEVEL			X	X	
CONTAINMENT SUMP LEVEL			X	X	
CONTAINMENT HUMIDITY				X	
CONTAINMENT RADIATION			X	X	X
CONTAINMENT HYDROGEN CONCENTRATION				X	
STEAM GENERATOR BLOWDOWN RADIATION			X		X
CONDENSER OFF-GAS RADIATION			X		X
MAIN STEAM LINE RADIATION			X		X

THE TRENDS/AIDS DISPLAY PARAMETER SUBSET INCLUDES ALL OF THE PARAMETERS NECESSARY TO MONITOR THESE CRITICAL SAFETY FUNCTIONS



A STUDY WAS CONDUCTED TO ASSESS THE CONSISTENCY BETWEEN THE ERF COMPUTER SYSTEM PARAMETER SET AND THE CPSES EMERGENCY RESPONSE GUIDELINES

BASIC METHOD



THIS ASSESSMENT COMPARED THE NOTED PARAMETERS WITH THE ERF COMPUTER SYSTEM PARAMETER SET

- THE TRENDS/AIDS DISPLAY PARAMETER SET INCLUDES ALL OF THE PARAMETERS NECESSARY TO MONITOR THE CRITICAL SAFETY FUNCTIONS

- THE TRENDS/AIDS DISPLAY PARAMETER SET WILL INCLUDE ALL OF THE PARAMETERS NECESSARY TO MONITOR THE SITE-SPECIFIC FUNCTIONAL RESTORATION GUIDELINES

- THE ERF COMPUTER SYSTEM PARAMETER SET INCLUDES ESSENTIALLY ALL OF THE PARAMETERS NECESSARY TO MONITOR ERG ENTRY/EXIT CONDITIONS

TWO OF THE PARAMETERS NECESSARY TO MONITOR ERG ENTRY/EXIT CONDITIONS ARE NOT INDICATED ON SYSTEM DISPLAYS, BUT MAY BE INFERRED FROM OTHER INDICATIONS

PRESSURIZER PORV BLOCK VALVE POSITION

- MAY BE INFERRED FROM INDICATIONS OF PRESSURIZER PRESSURE, PORV POSITION, AND PRESSURIZER RELIEF TANK TEMPERATURE AND PRESSURE

CONTAINMENT SUMP RECIRCULATION VALVE POSITION

- MAY BE INFERRED FROM CONTAINMENT SUMP LEVEL, REFUELING WATER STORAGE TANK LEVEL, RHR PUMP STATUS, AND RHR FLOW RATE

TWO CONCLUSIONS WERE DRAWN FROM THIS ASSESSMENT

- PARAMETERS PRESENTED ON THE TOP-LEVEL AND TRENDS/AIDS DISPLAYS ARE SUFFICIENT TO MEET THE INTENT OF NUREG-0696 AND NUREG-0737, SUPP. 1

- PARAMETER AVAILABILITY FOR THE ENTIRE ERF COMPUTER SYSTEM SUPPORTS AND IS COMPATIBLE WITH THE CPSES EMERGENCY RESPONSE GUIDELINE PROCEDURES

SUMMARY

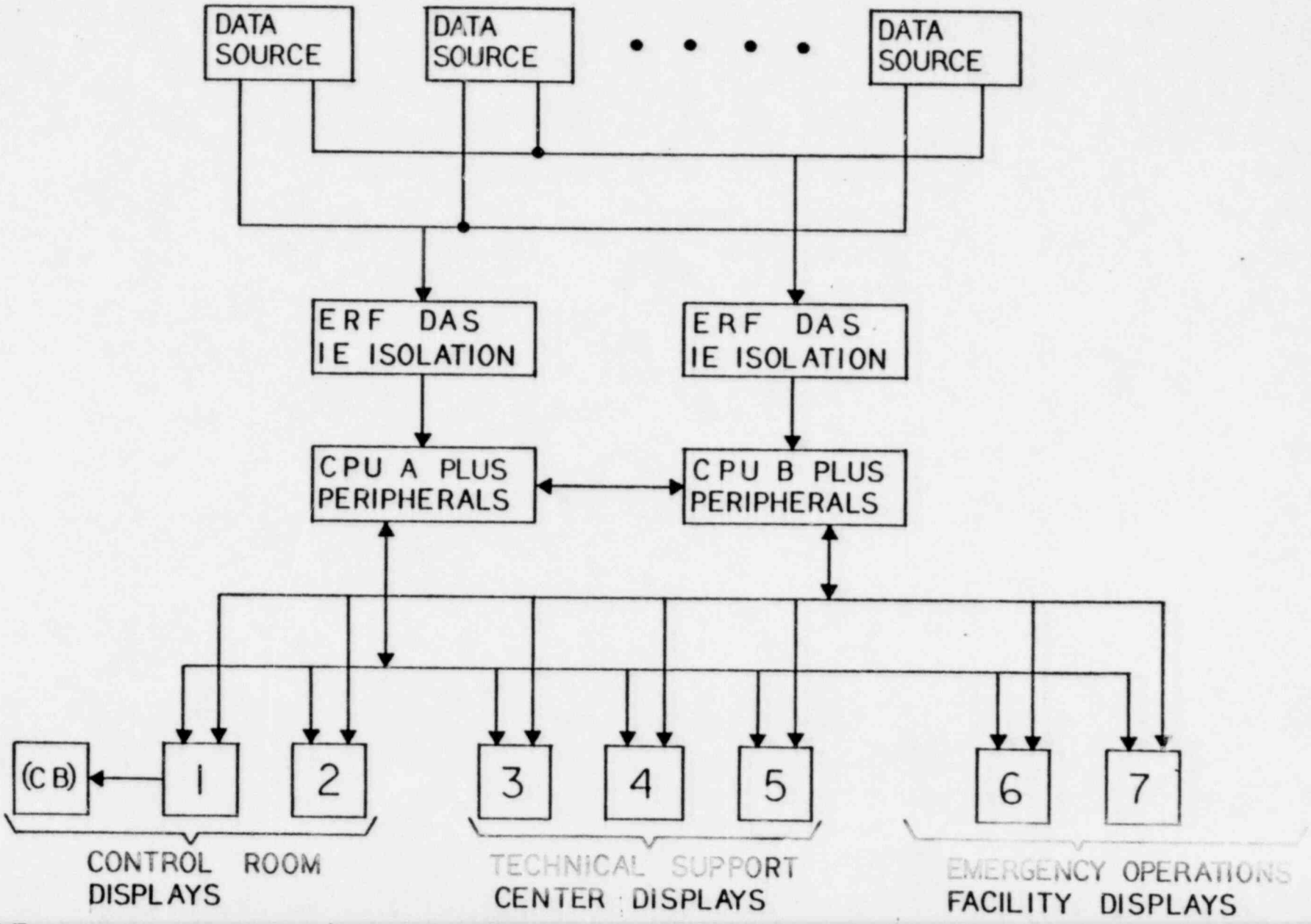
THE ERF COMPUTER SYSTEM PARAMETER SET HAS BEEN VALIDATED.

- IT INCLUDES AND PRESENTS ON THE TOP LEVEL DISPLAY THE SPDS PARAMETER SET VALIDATED IN THE GENERIC S.A.S. PROGRAM

- IT INCLUDES ALL OF THE PARAMETERS NECESSARY TO MONITOR THE CRITICAL SAFETY FUNCTIONS AND IMPLEMENT THE FUNCTION RESTORATION GUIDELINES

- ALL PARAMETERS NECESSARY TO MONITOR ENTRY AND EXIT POINTS IN THE CPSES EMERGENCY RESPONSE GUIDELINES EITHER ARE INDICATED ON SYSTEM DISPLAYS OR MAY BE INFERRED FROM OTHER INDICATIONS

HIGH SYSTEM AVAILABILITY HAS BEEN DESIGNED INTO THE SYSTEM.



DESIGN FEATURES

OF THE

SAFETY PARAMETER DISPLAY SYSTEM

AT THE

COMANCHE PEAK STEAM ELECTRIC STATION

PRESENTED TO THE

NRC AUDIT TEAM

ON

JUNE 25, 1985

BY

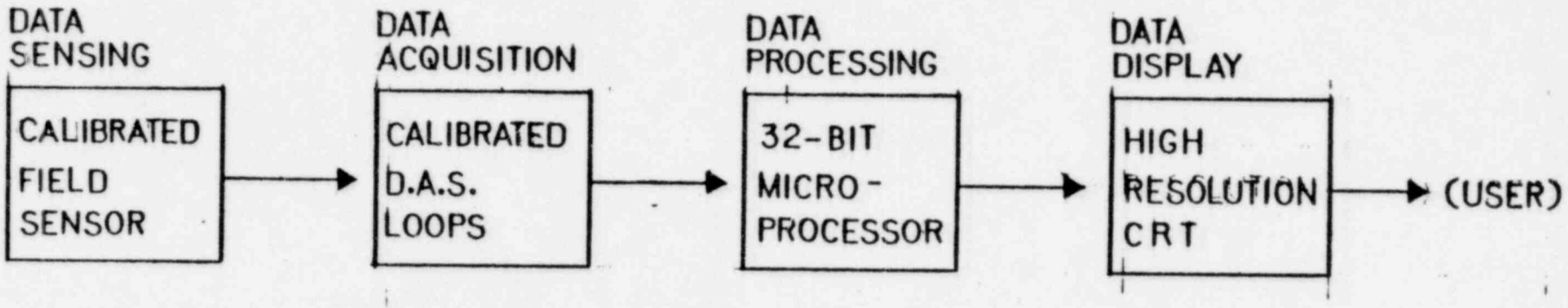
MARK A. COFFING

TUGCo NUCLEAR ENGINEERING

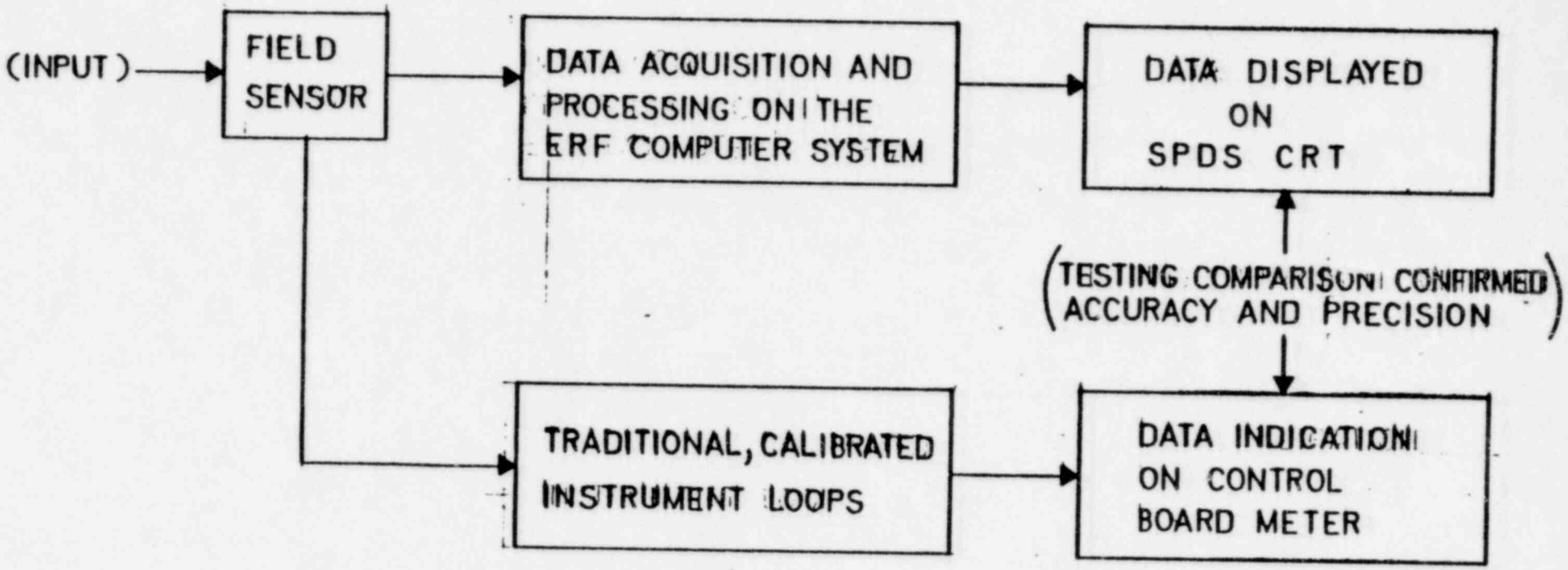
THE C.P.S.E.S. SAFETY PARAMETER DISPLAY SYSTEM HAS BEEN DESIGNED TO PROVIDE THE USER WITH DISPLAYS THAT WILL AID HIM IN RAPIDLY AND RELIABLY DETERMINING THE SAFETY STATUS OF THE PLANT DURING NORMAL, ABNORMAL, AND EMERGENCY CONDITIONS.

- CRT-BASED DISPLAYS PRESENT VALID CRITICAL PLANT VARIABLES
- THE SYSTEM IS DESIGNED TO ACHIEVE HIGH AVAILABILITY
- DISPLAYS INCORPORATE APPROPRIATE H.F.E. GUIDANCE

THE ACCURACY OF THE DATA PRESENTED TO THE USER IS ENSURED BY RIGOROUS CALIBRATION PROCEDURES AND HIGH-PRECISION COMPUTERS.



ACCURACY AND PRECISION WERE CONFIRMED THROUGH TESTING.



DATA VALIDATION IS ACCOMPLISHED THROUGH SYSTEM DESIGN FEATURES.

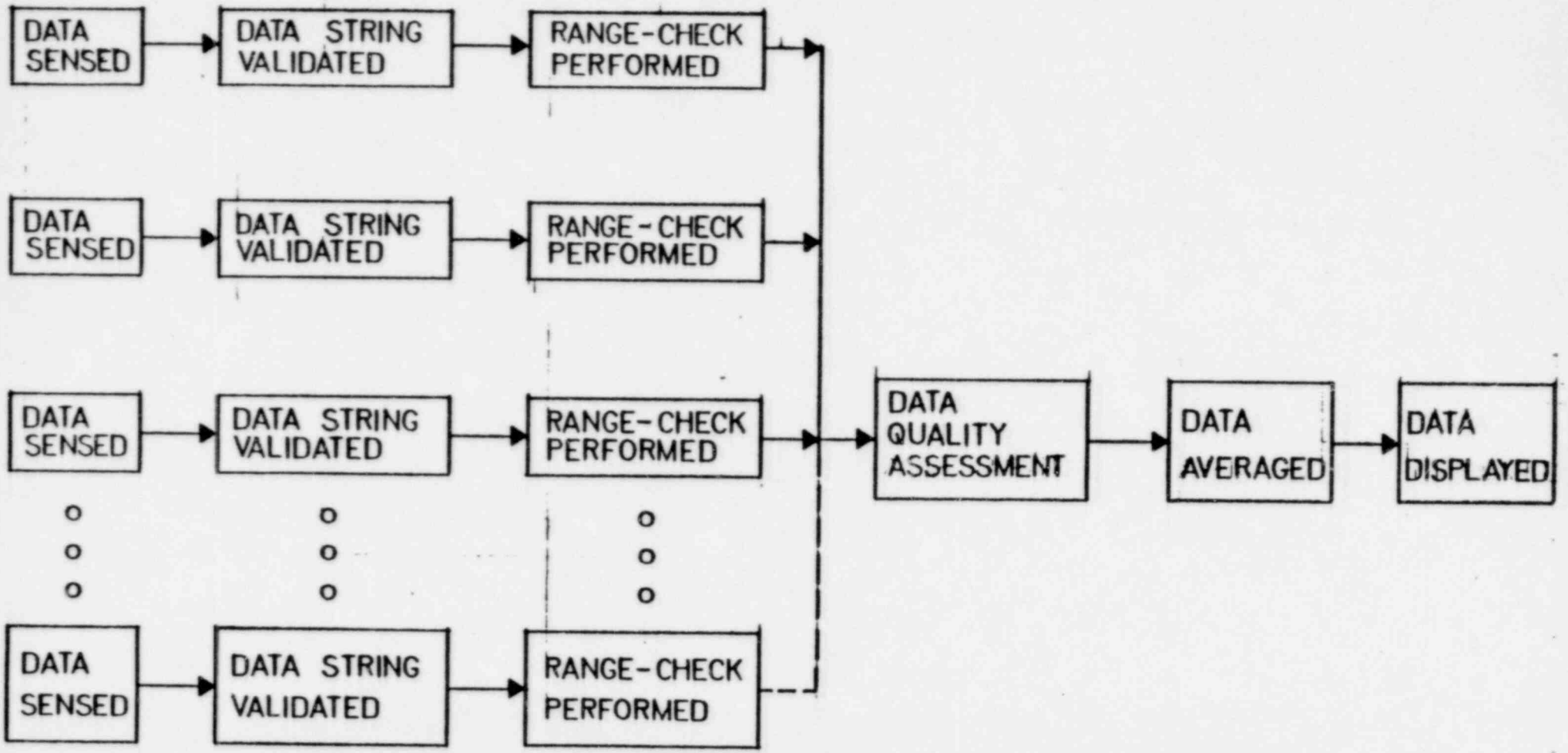
- DISPLAY FEATURES INDICATE VALIDITY
- EACH PARAMETER IS "RANGE-CHECKED"
- REDUNDANT PARAMETERS ARE COMPARED

DATA VALIDITY IS INDICATED ON THE DISPLAYS

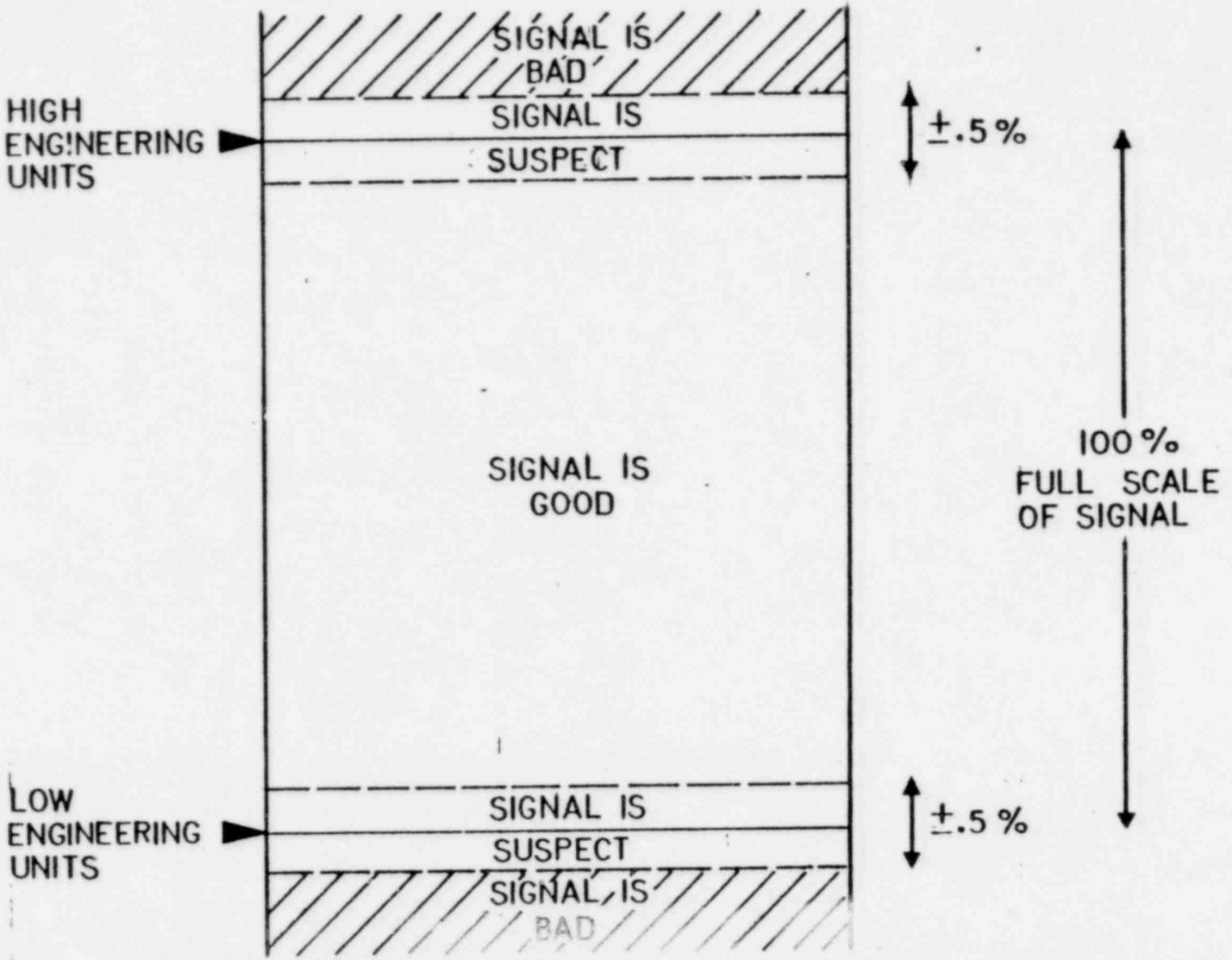
VALIDITY CONVENTIONS

GOOD DATA:	710	(WHITE TEXT)
SUSPECT DATA:	710	(WHITE TEXT YELLOW BOX)
BAD DATA:	****	(YELLOW ASTERISKS)

THE DATA VALIDATION METHODOLOGY INCLUDES SEVERAL DIFFERENT PROCESSES.



A KEY STEP IN DATA VALIDATION IS RANGE-CHECKING.



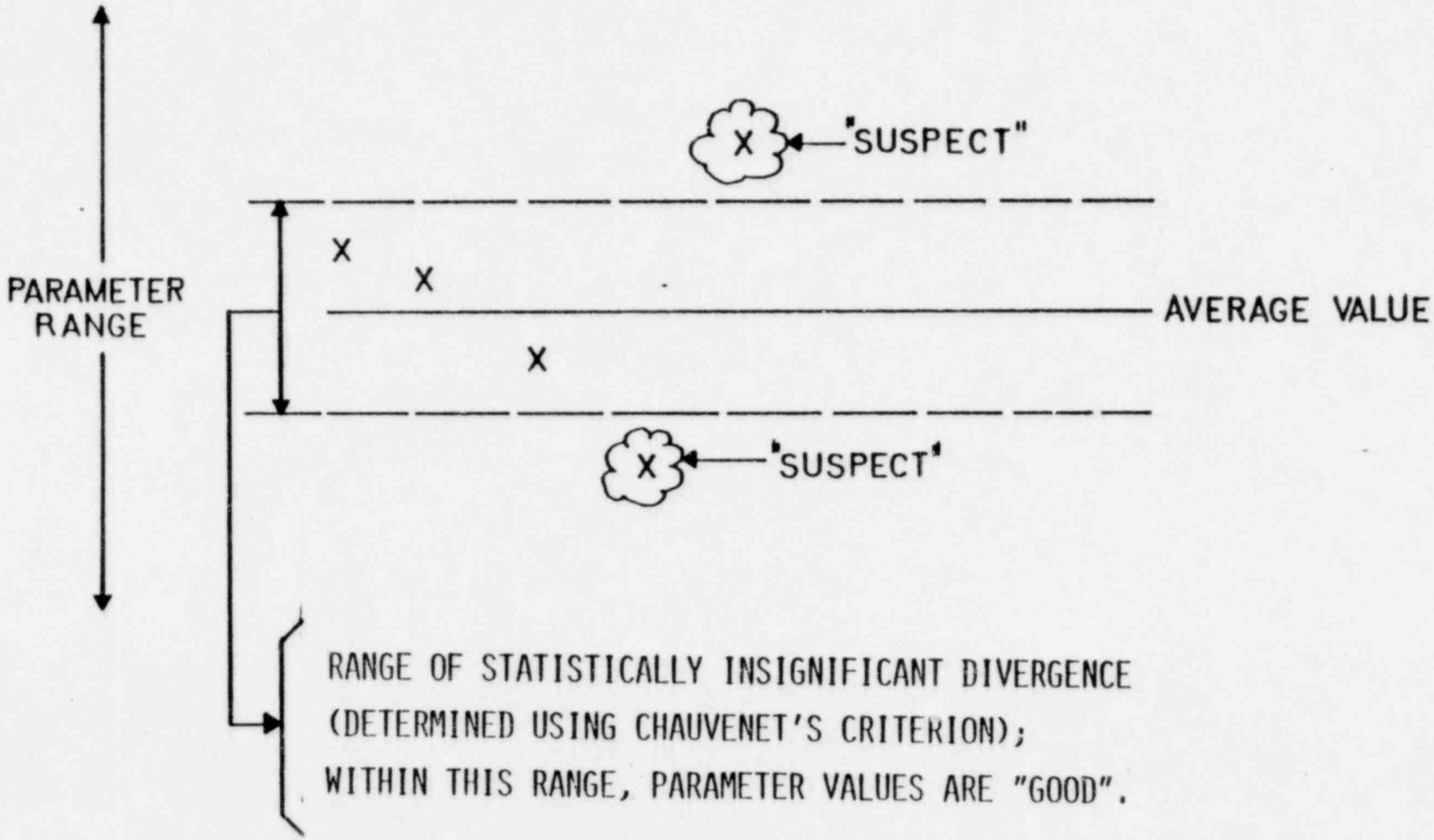
FOR PARAMETERS MONITORED BY ONE SENSOR, RANGE-CHECKING ALONE DETERMINES DATA VALIDITY.

RANGE CHECK RESULT	DISPLAY CONVENTION
GOOD	GOOD
SUSPECT	SUSPECT
BAD	BAD

FOR PARAMETERS DETERMINED BY TWO INPUT SENSORS, THE DISPLAY CONVENTION IS DETERMINED BY RANGE-CHECKING AND SIGNAL DIVERGENCE.

RESULTS OF RANGE-CHECKING			
SENSOR 1	SENSOR 2	DIVERGENCE	DISPLAY CONVENTION
GOOD	GOOD	$<$ 10%	GOOD
		$\geq$ 10%	SUSPECT
GOOD	SUSPECT	N/A	SUSPECT
GOOD	BAD	N/A	SUSPECT
SUSPECT	SUSPECT	N/A	SUSPECT
SUSPECT	BAD	N/A	SUSPECT
BAD	BAD	N/A	BAD

MULTIPLE-SENSOR DATA VALIDATION EMPLOYS CHAUVENET'S CRITERION TO IDENTIFY STATISTICALLY SIGNIFICANT DIVERGENCE.



MULTIPLE-SENSOR DATA VLAIDATION USES FEATURES
FROM THE SINGLE AND DUAL SENSOR DATA VALIDATION

FOR "N" SENSORS

MULTIPLE-SENSOR DATA (≥ 3)			
NUMBER GOOD	NUMBER SUSPECT	NUMBER BAD	DISPLAY CONVENTION
$N \geq 3$	ANY	ANY	GOOD
2	ANY	ANY	USES 2 INPUT CRITERIA
1	ANY	ANY	SUSPECT
0	≥ 1	ANY	SUSPECT
0	0	N	BAD

THE C.P.S.E.S. SAFETY PARAMETER DISPLAY SYSTEM HAS BEEN DESIGNED TO PROVIDE THE USER WITH DISPLAYS THAT WILL AID HIM IN RAPIDLY AND RELIABLY DETERMINING THE SAFETY STATUS OF THE PLANT DURING NORMAL, ABNORMAL, AND EMERGENCY CONDITIONS.

- CRT-BASED DISPLAYS PRESENT VALID CRITICAL PLANT VARIABLES
- ▶ THE SYSTEM IS DESIGNED TO ACHIEVE HIGH AVAILABILITY
- DISPLAYS INCORPORATE APPROPRIATE H.F.E. GUIDANCE

AVAILABILITY DESIGN GOAL

UNAVAILABILITY - NORMAL .01

- OLD SHTDN .20

PRIME 750	MTBF = 7449 HRS	(.00966)
DISK DRIVES	MTBF = 6695 HRS	(.01075)
EST. TTR	= 72 HRS	

- SINGLE SYSTEM NEAR CRITERIA

- DUAL SYSTEMS WITH AUTOMATIC FAILOVER

  -REQUIRES SIMULTANEOUS FAILURES TO TAKE THE SYSTEM DOWN.

- DUAL SYSTEMS ALLOW OPERATIONAL FLEXIBILITY.

  -CODE UPGRADES

  -SPECIAL ANALYSIS

  -OTHER ACTIVITIES

HIGH SYSTEM

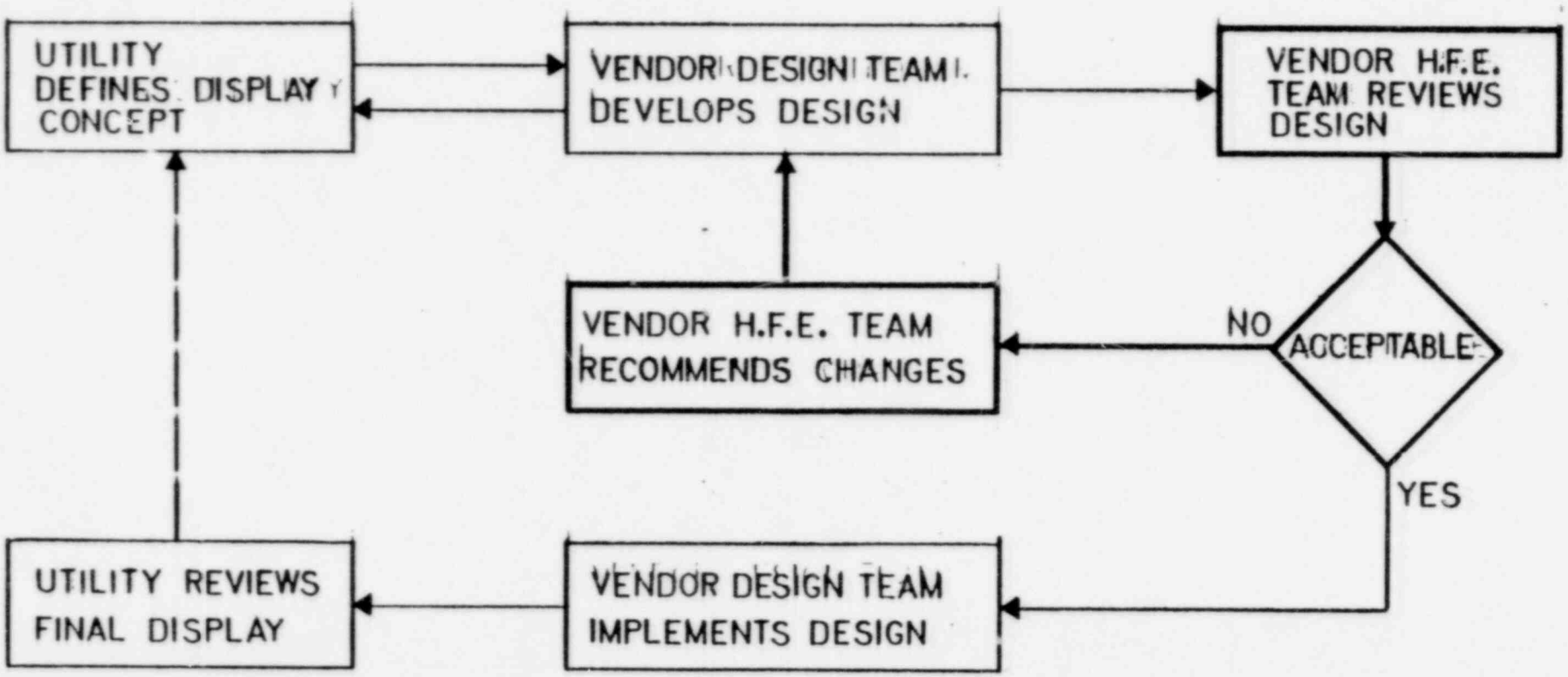
AVAILABILITY

THE C.P.S.E.S. SAFETY PARAMETER DISPLAY SYSTEM HAS BEEN DESIGNED TO PROVIDE THE USER WITH DISPLAYS THAT WILL AID HIM IN RAPIDLY AND RELIABLY DETERMINING THE SAFETY STATUS OF THE PLANT DURING NORMAL, ABNORMAL, AND EMERGENCY CONDITIONS.

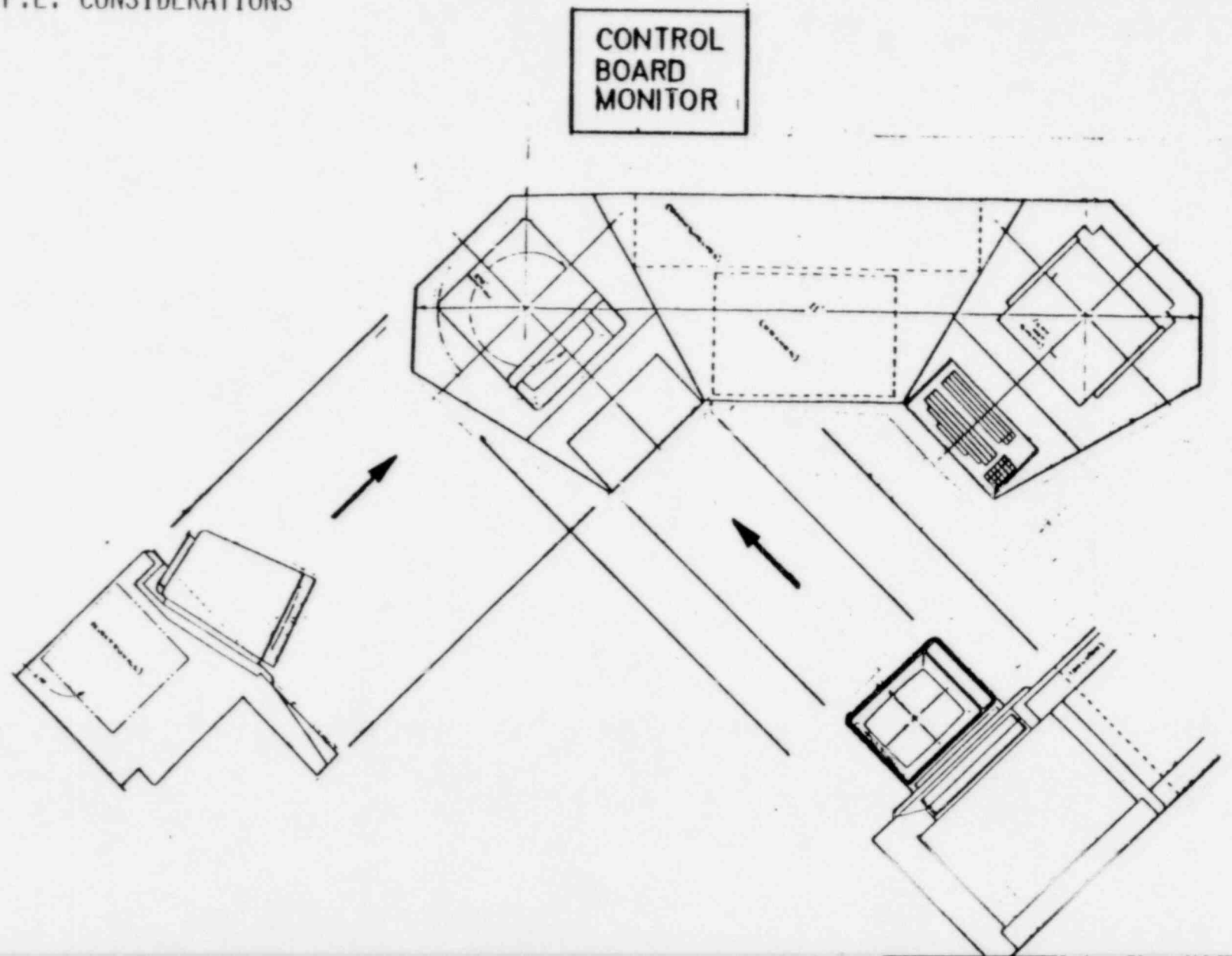
- CRT-BASED DISPLAYS PRESENT VALID CRITICAL PLANT VARIABLES
- THE SYSTEM IS DESIGNED TO ACHIEVE HIGH AVAILABILITY
- DISPLAYS INCORPORATE APPROPRIATE H.F.E. GUIDANCE

INCORPORATION OF H.F.E. CONCEPTS WAS AN INTEGRAL STEP IN DESIGN DEVELOPMENT.

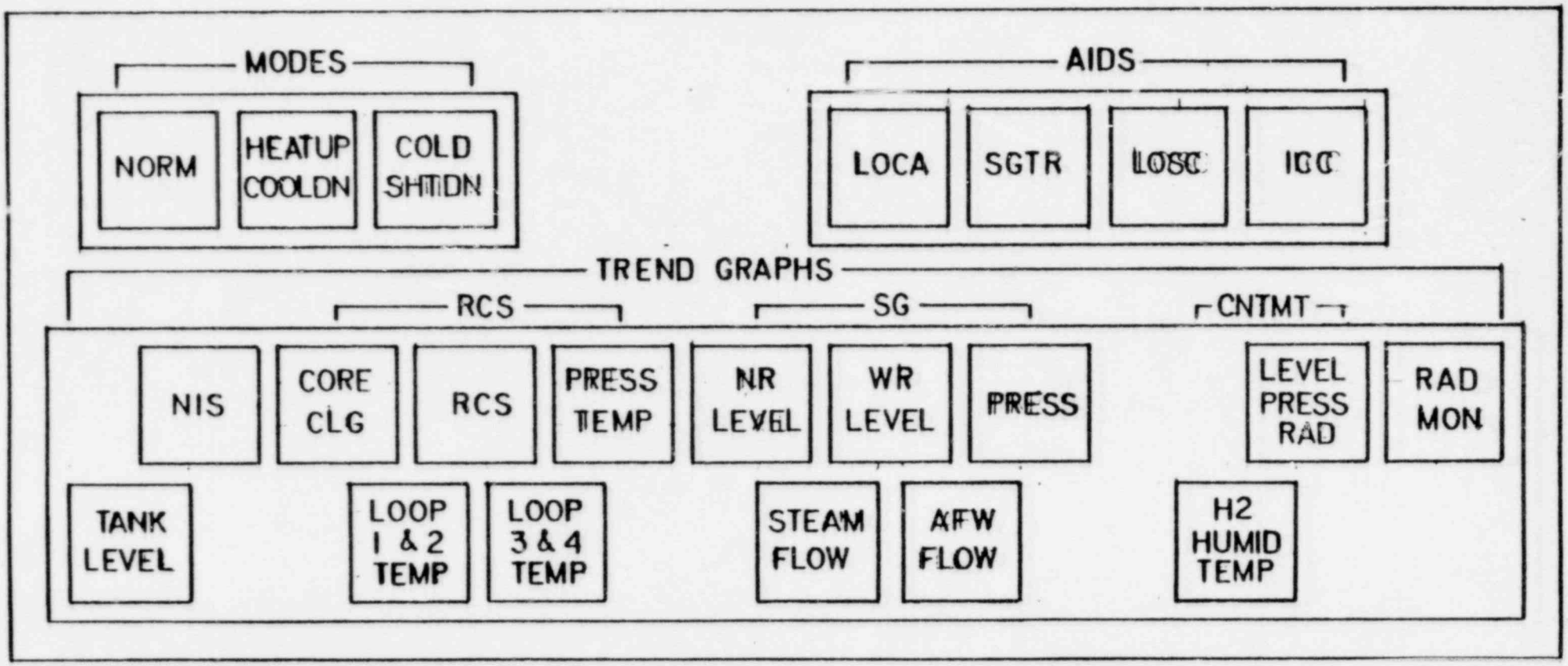
BASIC DESIGN CYCLE



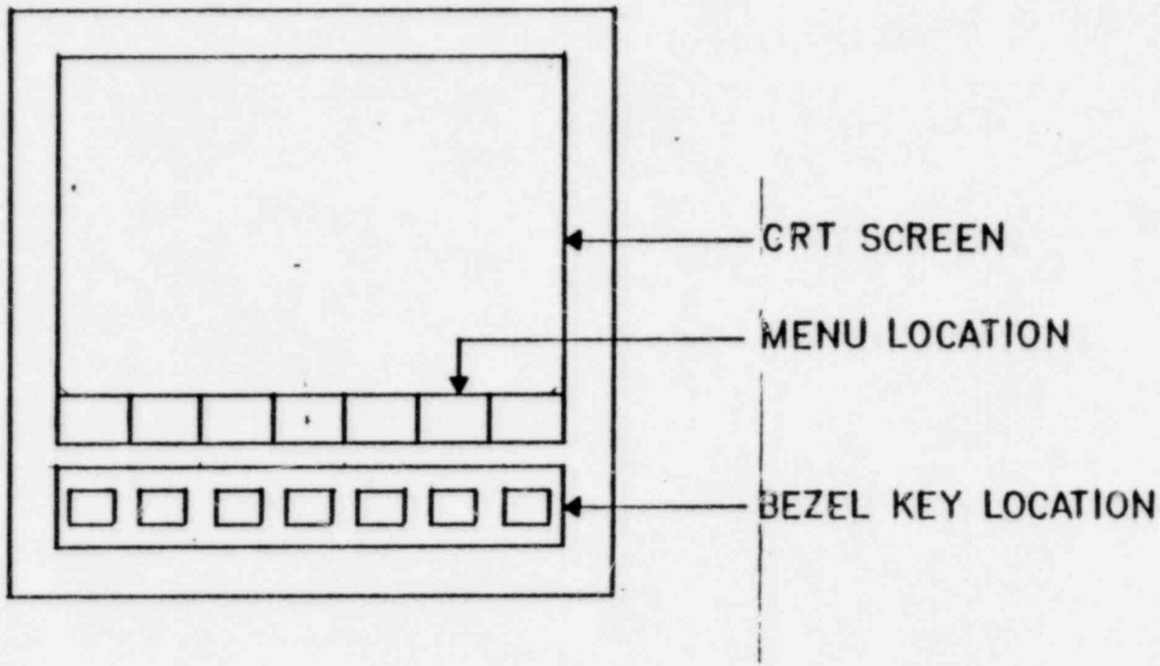
SPDS DISPLAYS ARE PRESENTED IN THE CONTROL ROOM ON A CONSOLE THAT INCORPORATES H.F.E. CONSIDERATIONS



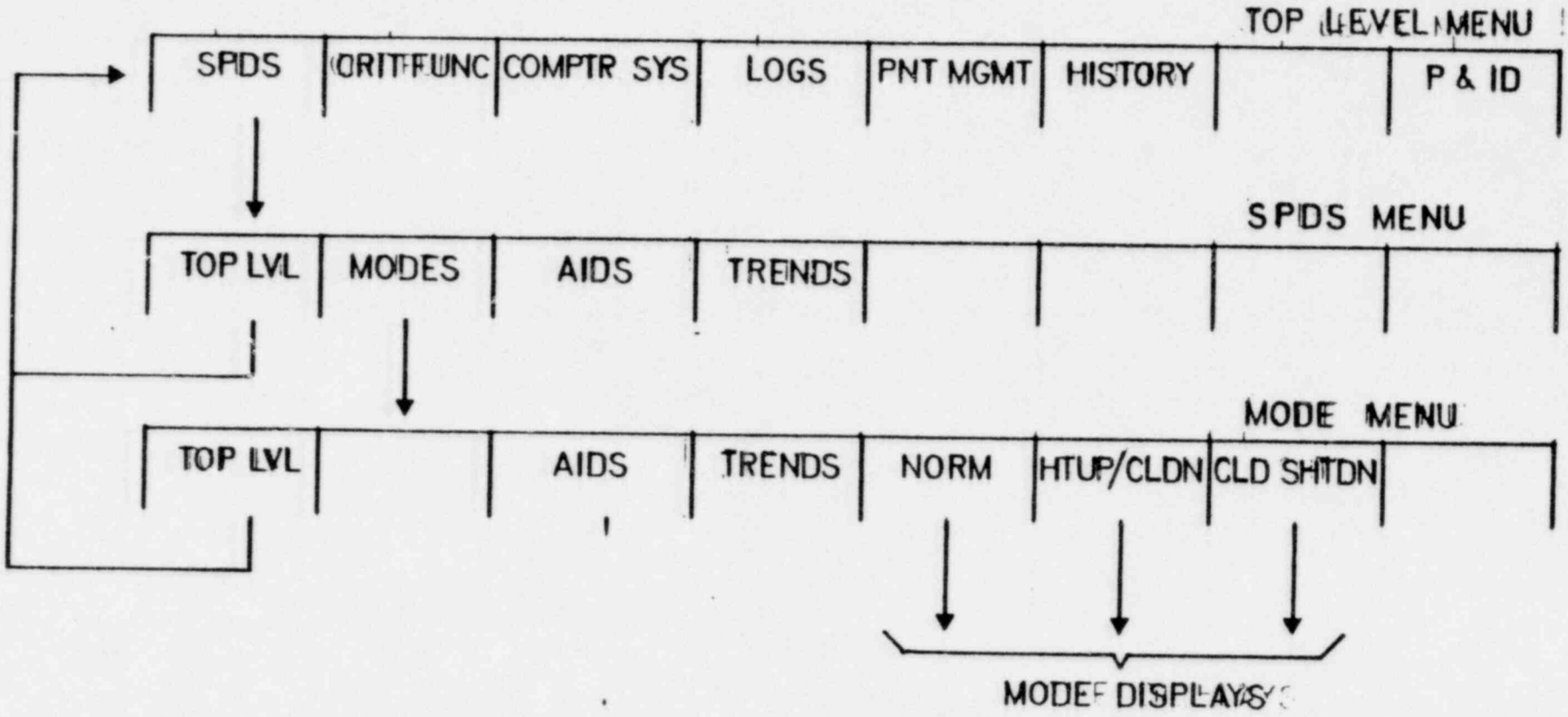
SPDS DISPLAYS ARE ACCESSED FROM THE OPERATOR'S C.R.T. AND THE CONTROL BOARD VIA A DEDICATED FUNCTION KEYPAD.



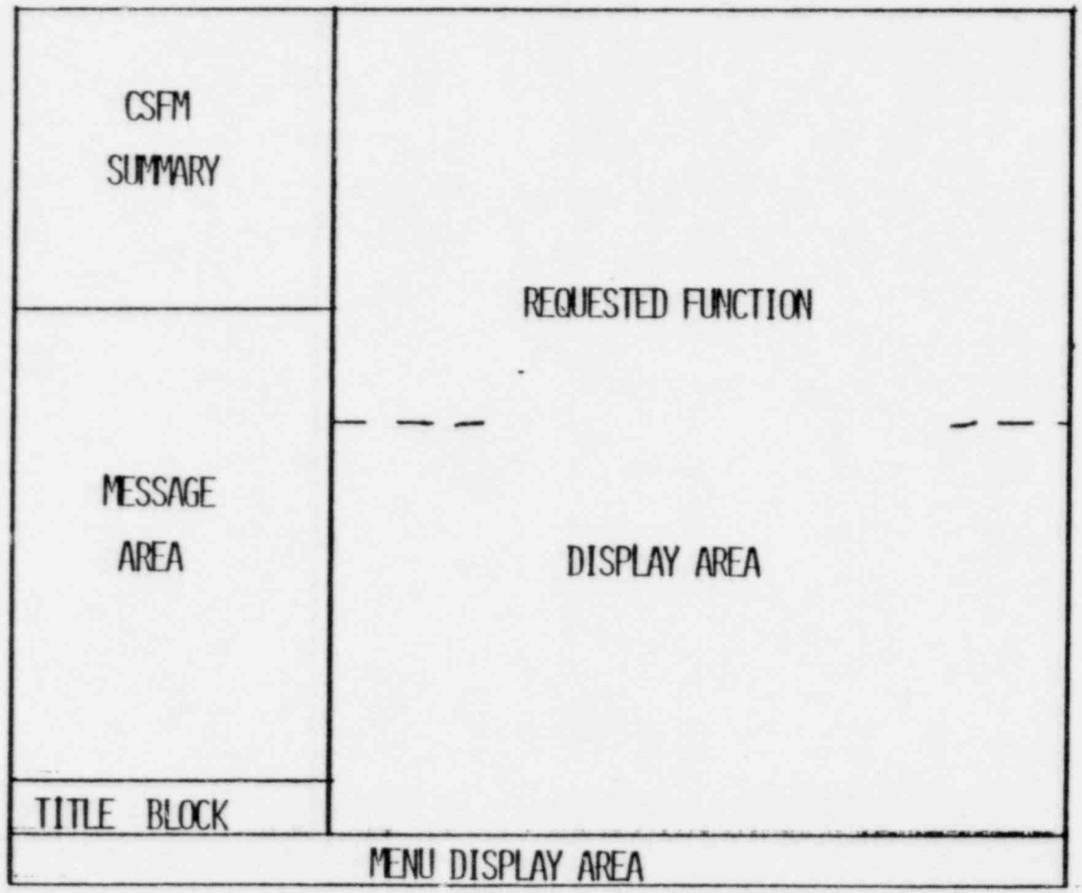
FROM ALL OTHER C.R.T.S., DISPLAYS ARE SELECTED BY USING BEZEL KEYS TO MOVE THROUGH A HEIRARCHICAL DISPLAY SELECTION MENU.



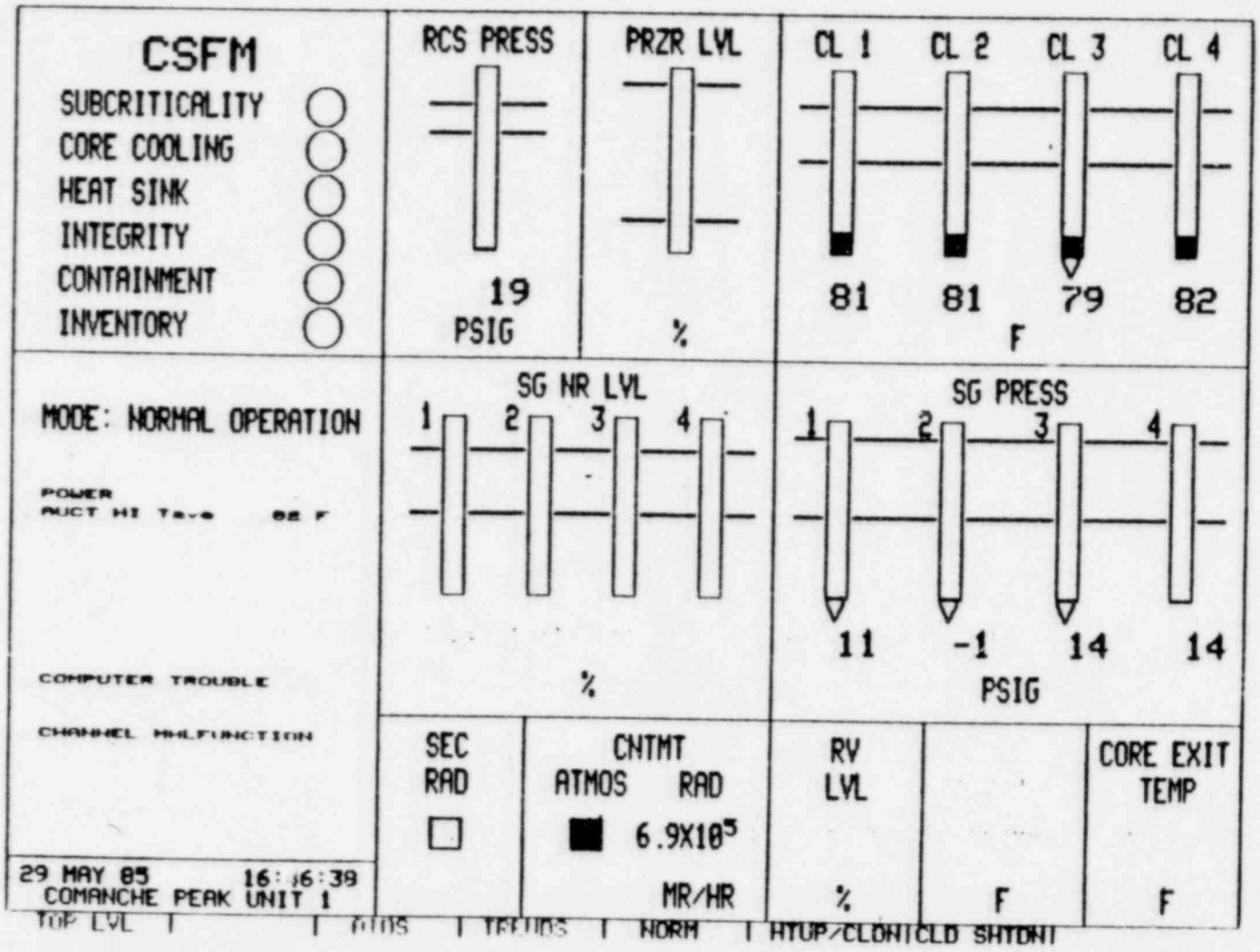
THE DISPLAY SELECTION MENU IS HEIRARCHICAL.



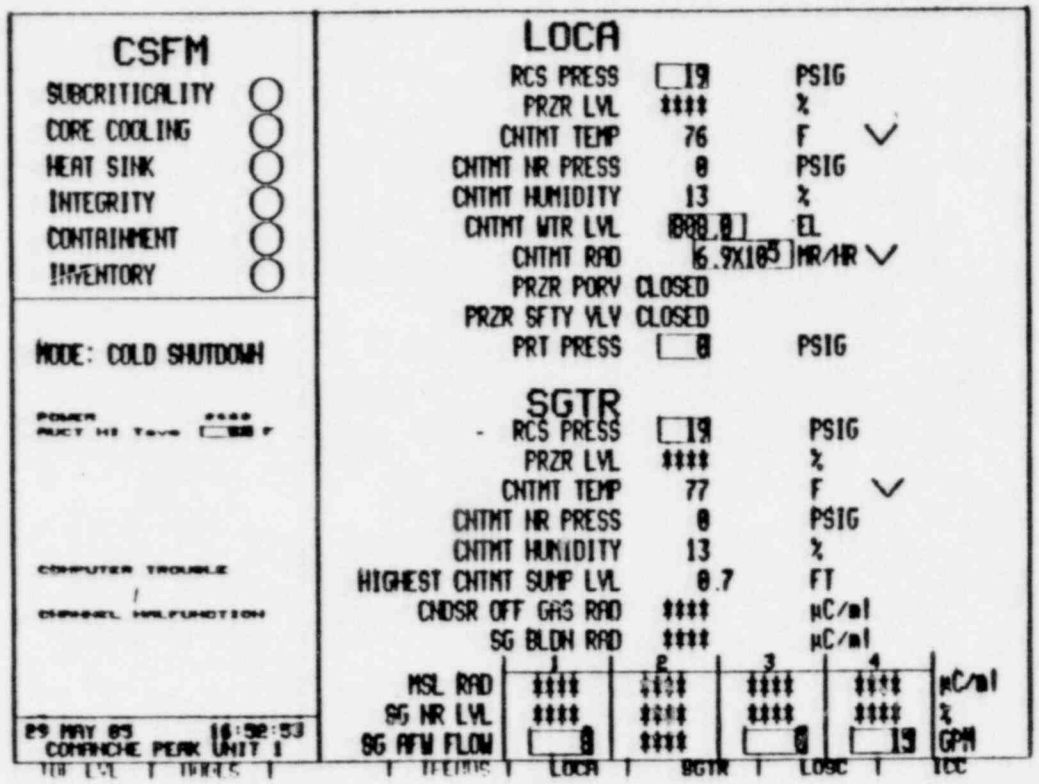
ALL SPDS DISPLAYS (EXCEPT THE TOP LEVEL COLD SHUTDOWN DISPLAY) ARE PATTERNED IN AN IDENTICAL FORMAT



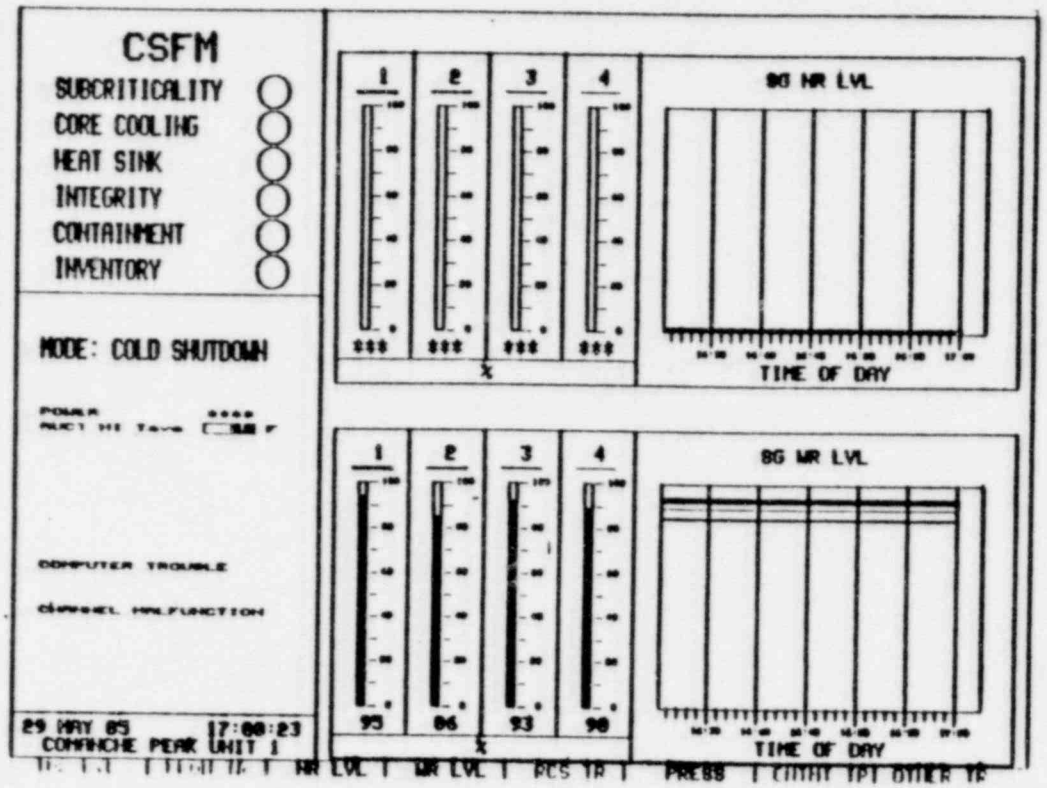
INCORPORATION OF H.F.E. CONCEPTS IS EVIDENT IN THE SPDS NORMAL OPERATIONS MODE DISPLAY.



ACCIDENT INDENTIFICATION DISPLAY SYSTEM (AIDS) DISPLAYS INCORPORATE SEVERAL H.F.E. CONSIDERATIONS.



H.F.E. CONCEPTS ARE ALSO EVIDENT IN THE DESIGN OF THE C.P.S.E.S. SPDS TREND GRAPHS.



SUMMARY

THE C.P.S.E.S. SAFETY PARAMETER DISPLAY SYSTEM PROVIDES THE USER WITH READABLE, COMPREHENSIBLE, AND ACCURATE DISPLAYS OF THE PLANT PARAMETERS.

- THE SPDS DESIGN ENSURES THAT THE DATA PRESENTED TO THE USER ARE ACCURATE AND VALID.

- THE SPDS IS DESIGNED TO ACHIEVE HIGH AVAILABILITY.

- THE SPDS DESIGN INCORPORATES APPROPRIATE H.F.E. CONCEPTS.

VERIFICATION & VALIDATION ACTIVITIES FOR THE C.P.S.E.S. UNIT 1 SAFETY PARAMETER DISPLAY SYSTEM

PRESENTED TO
THE NRC AUDIT TEAM
JUNE 25, 1985

BY
MARK A. COFFING
TUGCO NUCLEAR ENGINEERING

A COMPREHENSIVE VERIFICATION & VALIDATION PROGRAM HAS BEEN AN INTEGRAL PART OF THE ERF COMPUTER SYSTEM PROJECT.

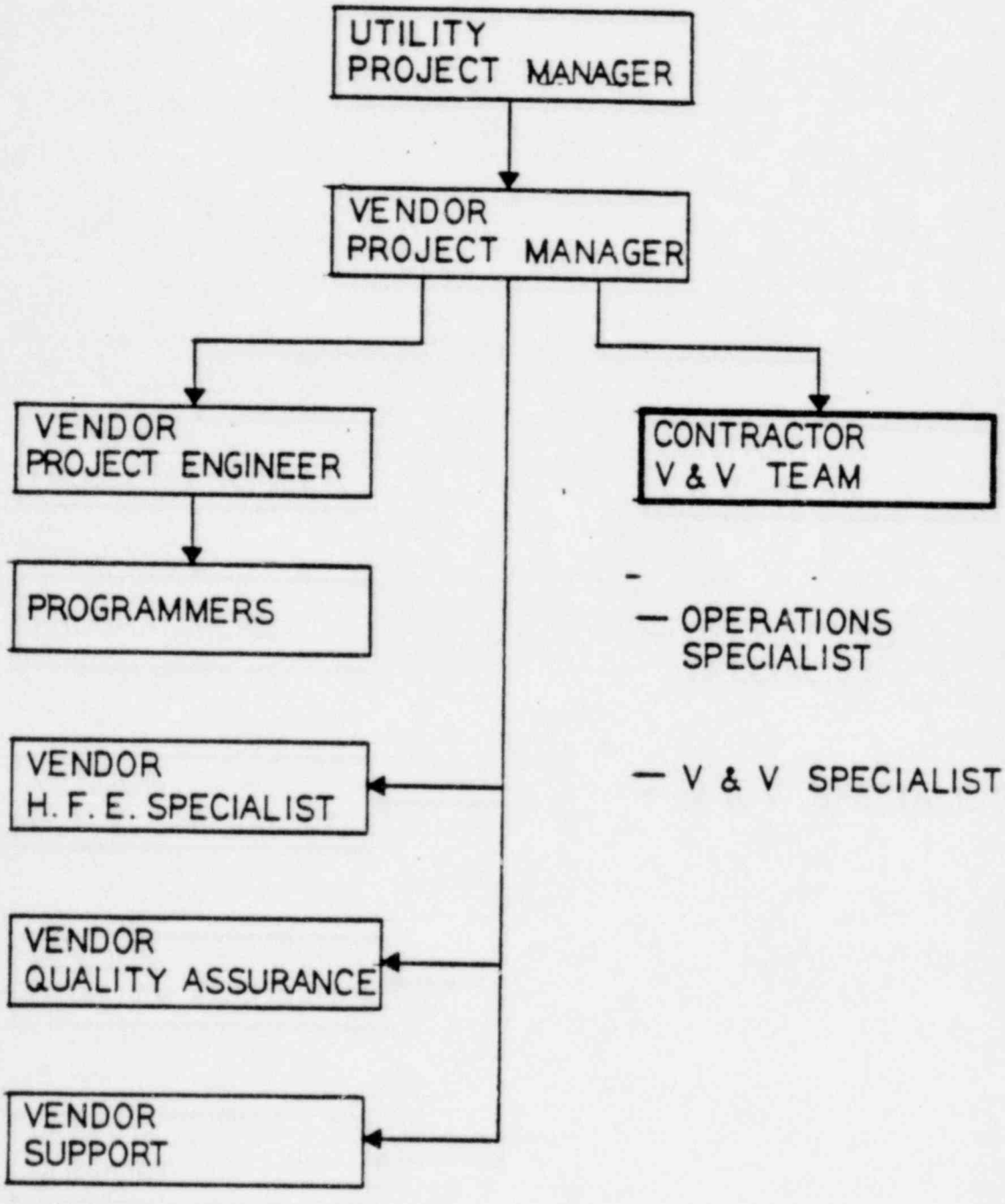
- THE V&V SCOPE ENCOMPASSED THE ENTIRE SYSTEM
- THE PROGRAM REQUIRED V&V TEAM PERSONNEL TO BE INDEPENDENT OF DESIGN EFFORTS
- THE PROGRAM WAS BASED ON NSAC-39 "VERIFICATION AND VALIDATION FOR SAFETY PARAMETER DISPLAY SYSTEMS"

THE V&V PROGRAM ENCOMPASSED THE ENTIRE ERF COMPUTER SYSTEM.

- INCLUDED, BUT NOT LIMITED TO, SPDS FEATURES
- INCLUDED ACTIVITIES TO ESTABLISH COMPLIANCE WITH:
    - REGULATORY GUIDANCE
    - FUNCTIONAL SPECIFICATIONS

V&V SERVICES WERE PROVIDED BY CONTRACT PERSONNEL WHO REMAINED INDEPENDENT OF DESIGN EFFORTS.

BASIC PROJECT ORGANIZATION

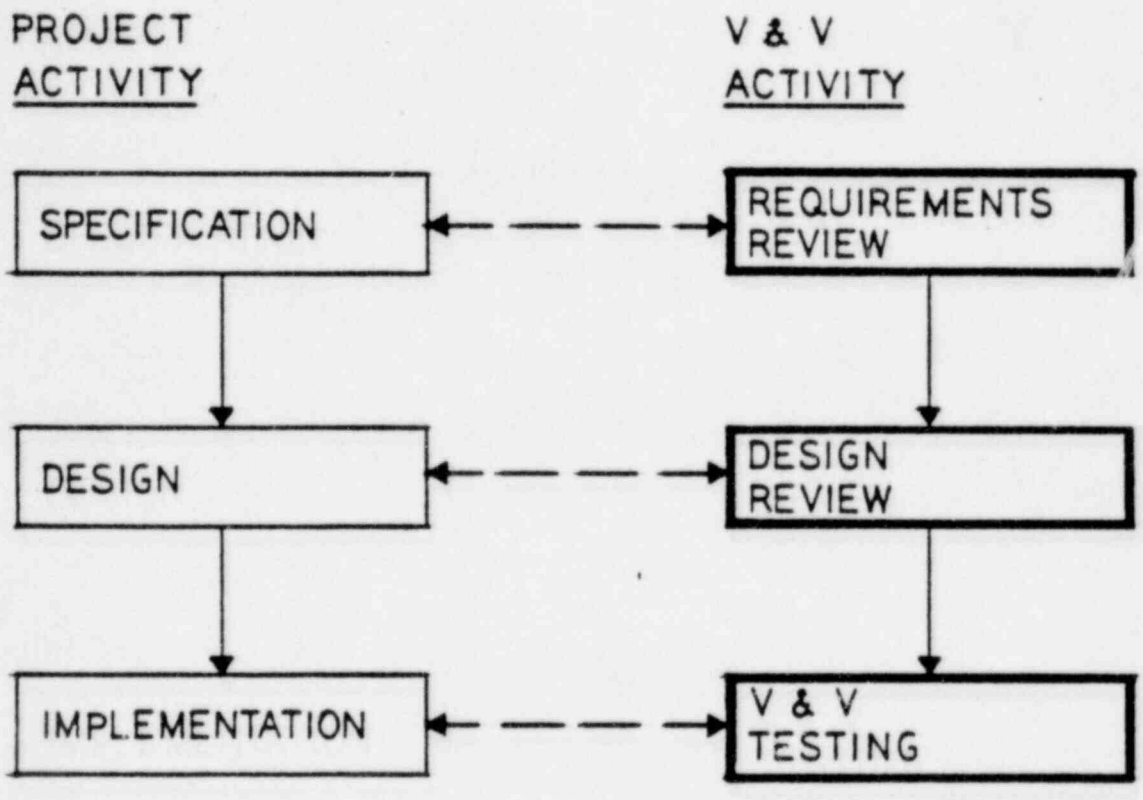


THE V&V PROGRAM INCLUDED ELEMENTS TO ESTABLISH COMPLIANCE WITH REGULATORY GUIDANCE AND FUNCTIONAL SPECIFICATIONS.

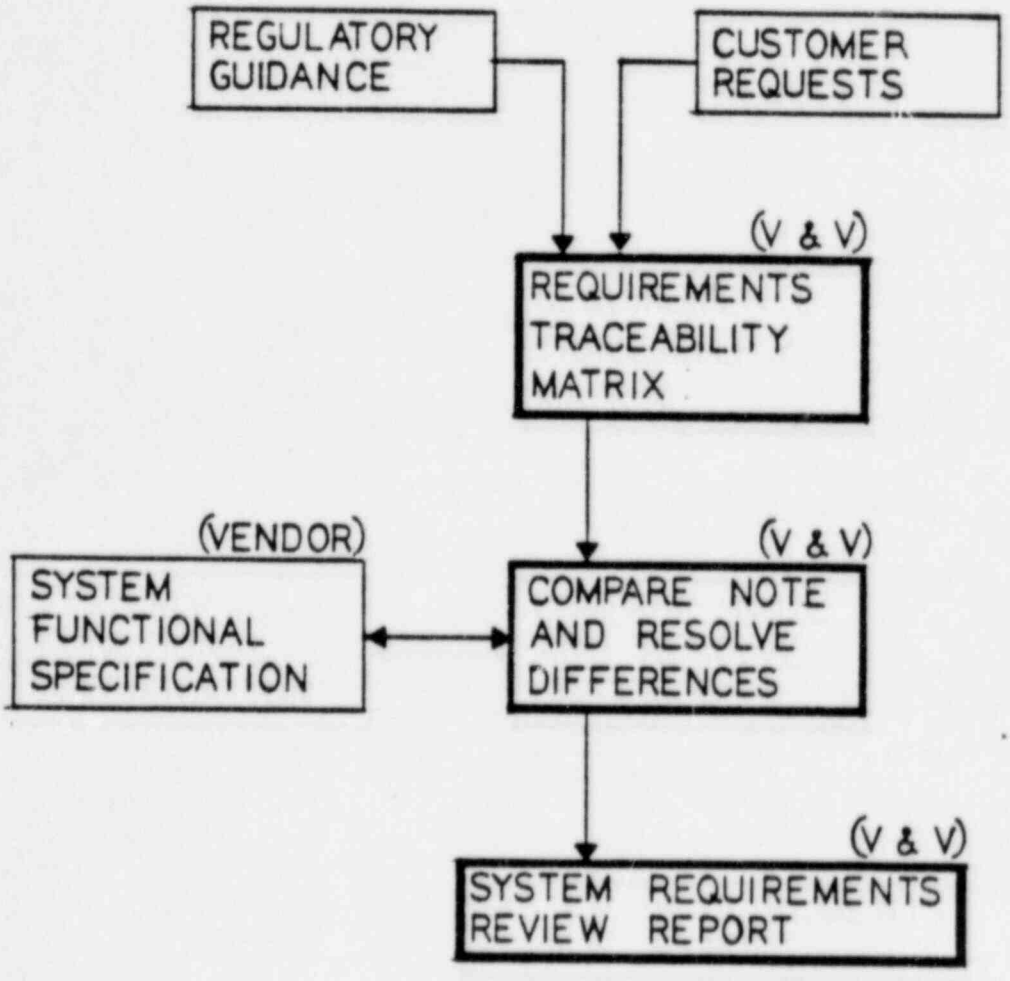
BASIC PROGRAM ELEMENTS

- SYSTEM REQUIREMENTS REVIEWS
- HARDWARE, SOFTWARE DESIGN REVIEWS
- V&V TESTING
- COMPREHENSIVE DOCUMENTATION

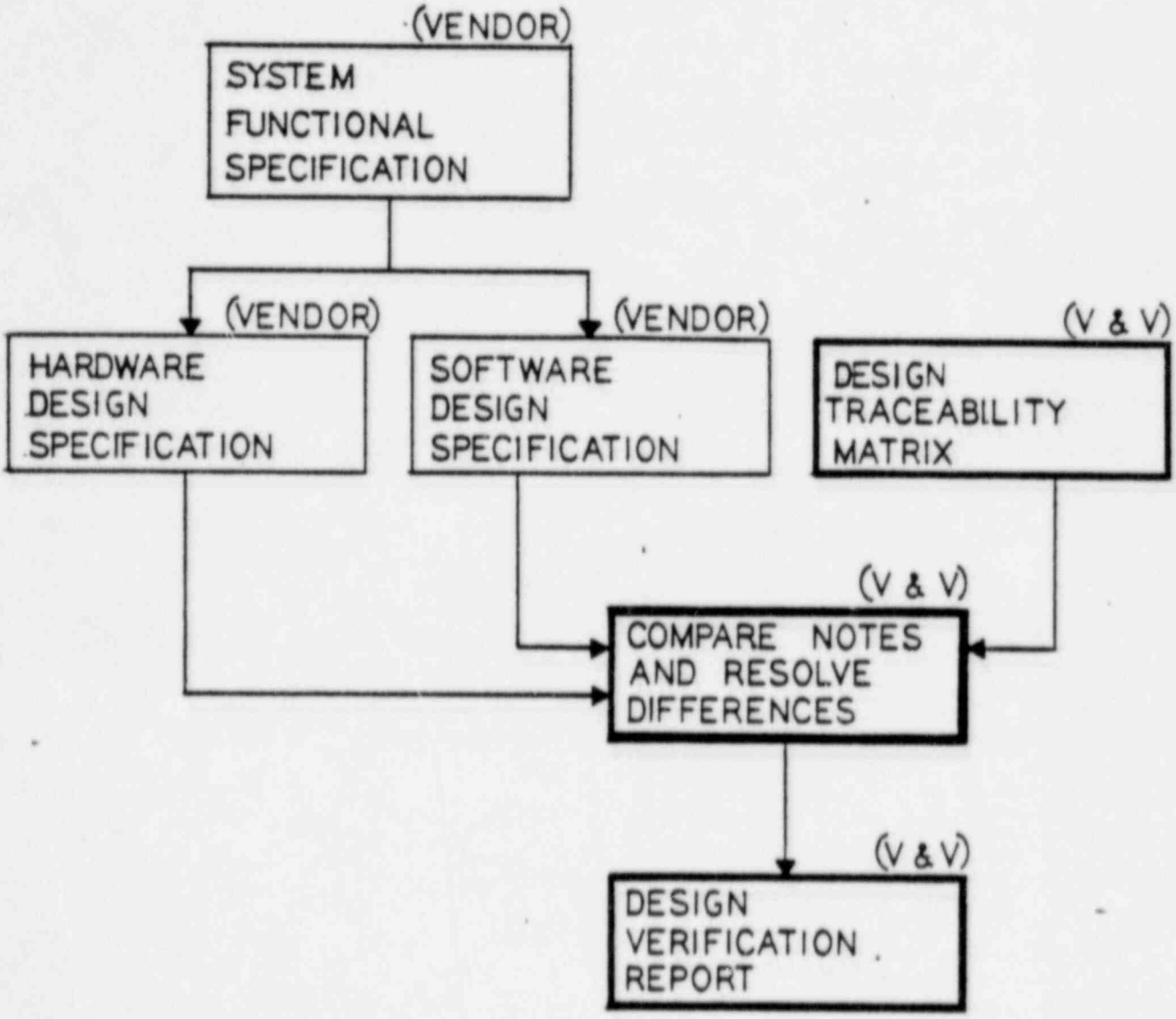
V&V ACTIVITIES FOR THE C.P.S.E.S. UNIT 1 SPDS INCLUDED SEVERAL ITERATIONS OF A SIMPLE SEQUENCE WHICH PARALLELED PROJECT ACTIVITIES.



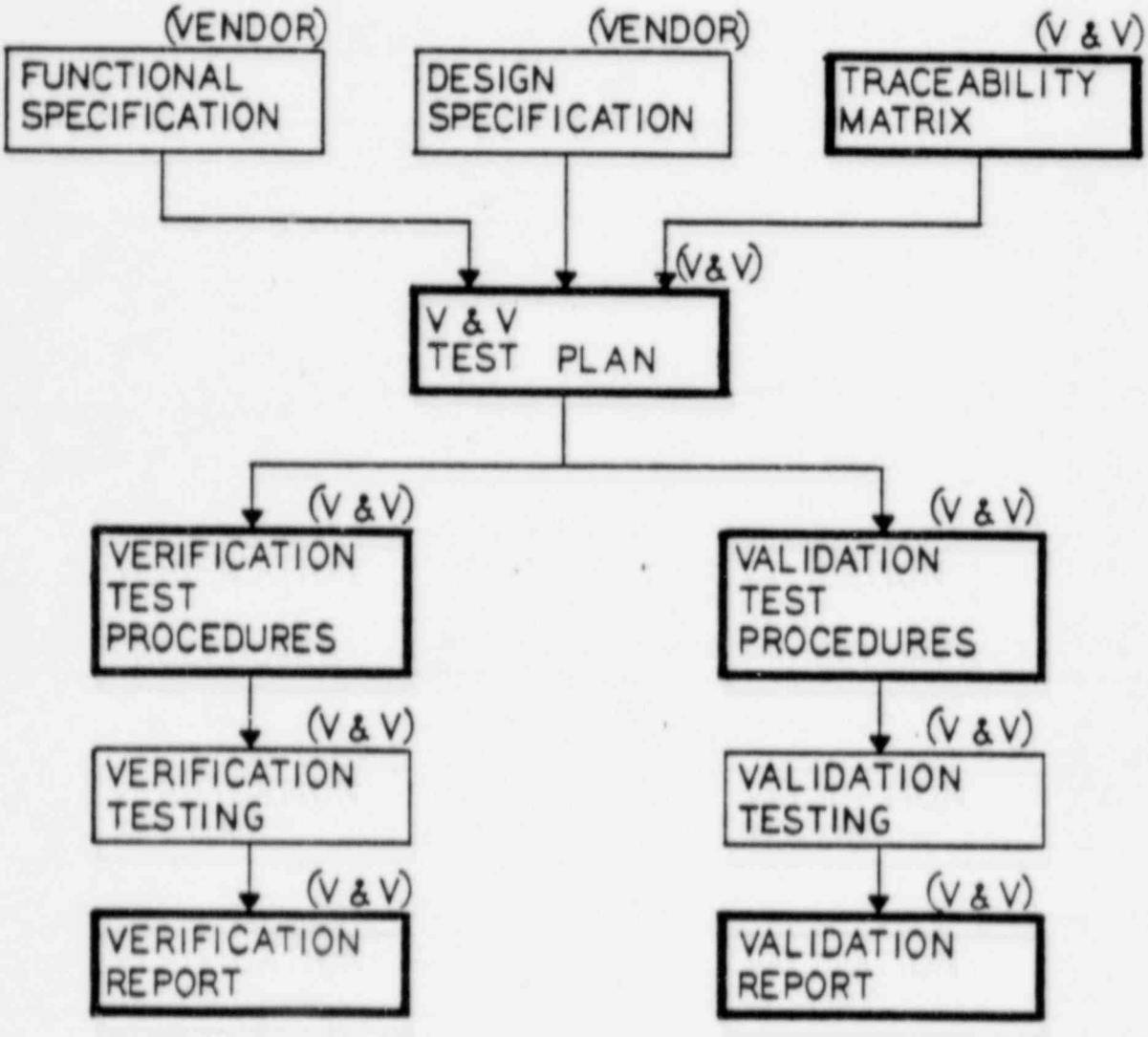
THE REQUIREMENTS REVIEW ACTIVITY ENSURED THE ADEQUACY OF THE SYSTEM FUNCTIONAL SPECIFICATIONS.



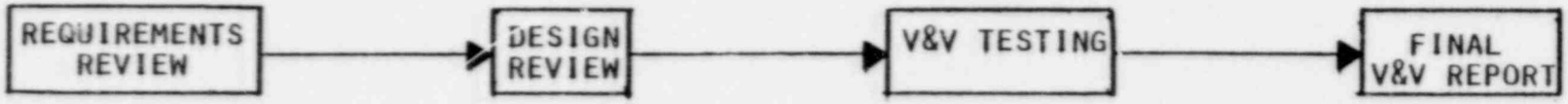
THE DESIGN REVIEW ACTIVITY ASSESSED THE ADEQUACY OF DESIGN SPECIFICATIONS.



THE V&V TESTING ACTIVITY VERIFIED IMPLEMENTATION OF THE DESIGN SPECIFICATIONS.



THERE WAS A LOGICAL SEQUENCE TO THE C.P.S.E.S. V&V ACTIVITIES.



- REGULATORY GUIDANCE
- FUNCTIONAL REQUIREMENTS
- REQUIREMENTS MATRIX

- HARDWARE & SOFTWARE SPECIFICATIONS
- DESIGN MATRIX

- TEST PLAN
- TEST PROCEDURE
- VALIDATION TEST
- VERIFICATION TEST
- MOD VERIFICATION
- PHASE 1½ TEST

THE BASIC V&V SEQUENCE WAS REPEATED SEVERAL TIMES.

	REQUIREMENTS REVIEW	DESIGN REVIEW	TESTING
VENDOR STAGING TEST	9/81	3/82	9/82
SITE STAGING TEST	12/82	6/83	8/83
SITE VALIDATION	8/83	8/83	10/83
SITE VERIFICATION	11/83	11/83	11/83
FINAL V & V	3/84	5/84	6/84
CSFM REVISIONS	1/85	3/85	3/85

SUMMARY

INDEPENDENT VERIFICATION & VALIDATION ACTIVITIES HAVE BEEN COMPLETED FOR THE UNIT 1 C.P.S.E.S. SPDS.

- REQUIREMENTS REVIEWS
- DESIGN REVIEWS
- V&V TESTING
- COMPREHENSIVE DOCUMENTATION

THE DOCUMENTATION AVAILABLE FOR REVIEW ON THE BACK TABLE IS:

V&V PROJECT PLAN

REQUIREMENTS REVIEW REPORT

DESIGN REVIEW REPORT

TEST REPORTS:

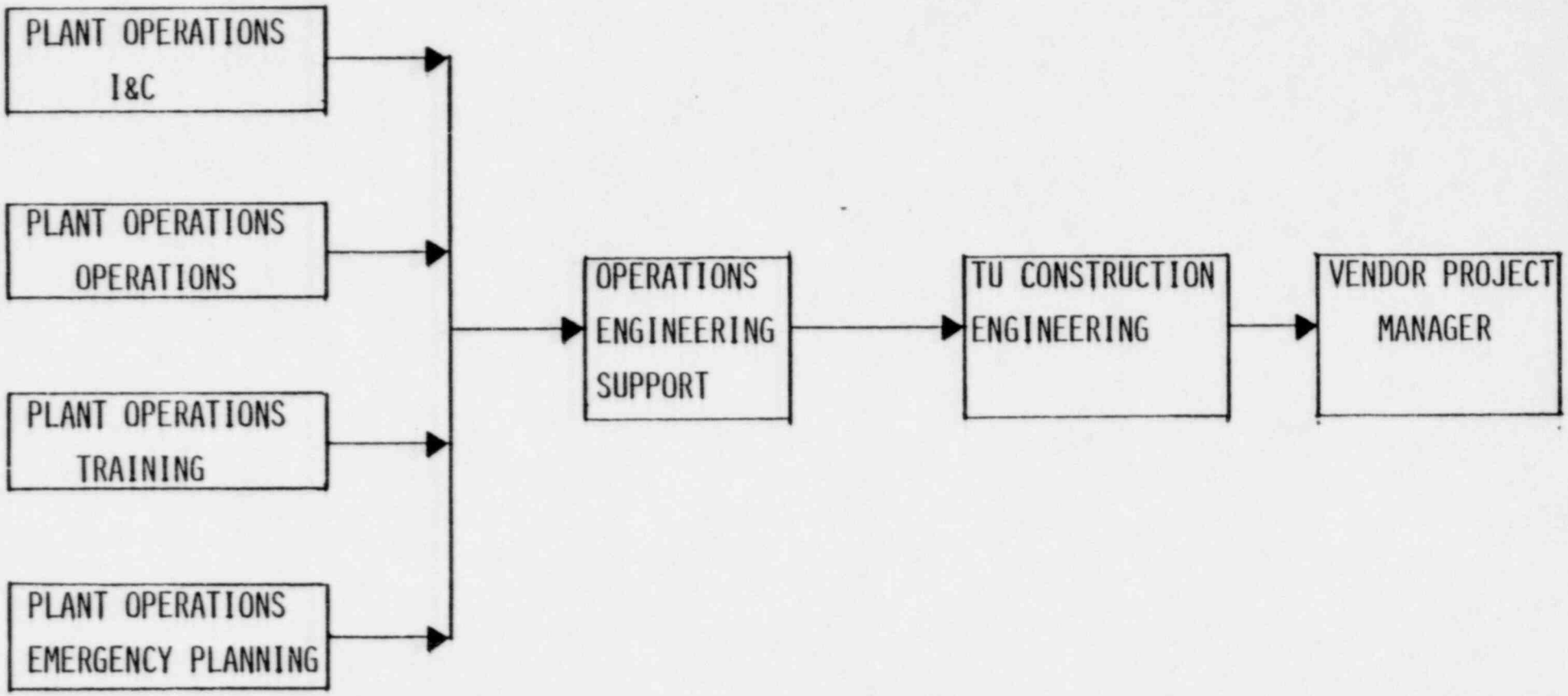
- VALIDATION TEST REPORT
- VERIFICATION TEST REPORT
- MOD 1 VERIFICATION TEST REPORT
- PHASE 1½ VERIFICATION TEST REPORT

FINAL V&V REPORT

GENERIC S.A.S. DOCUMENTS

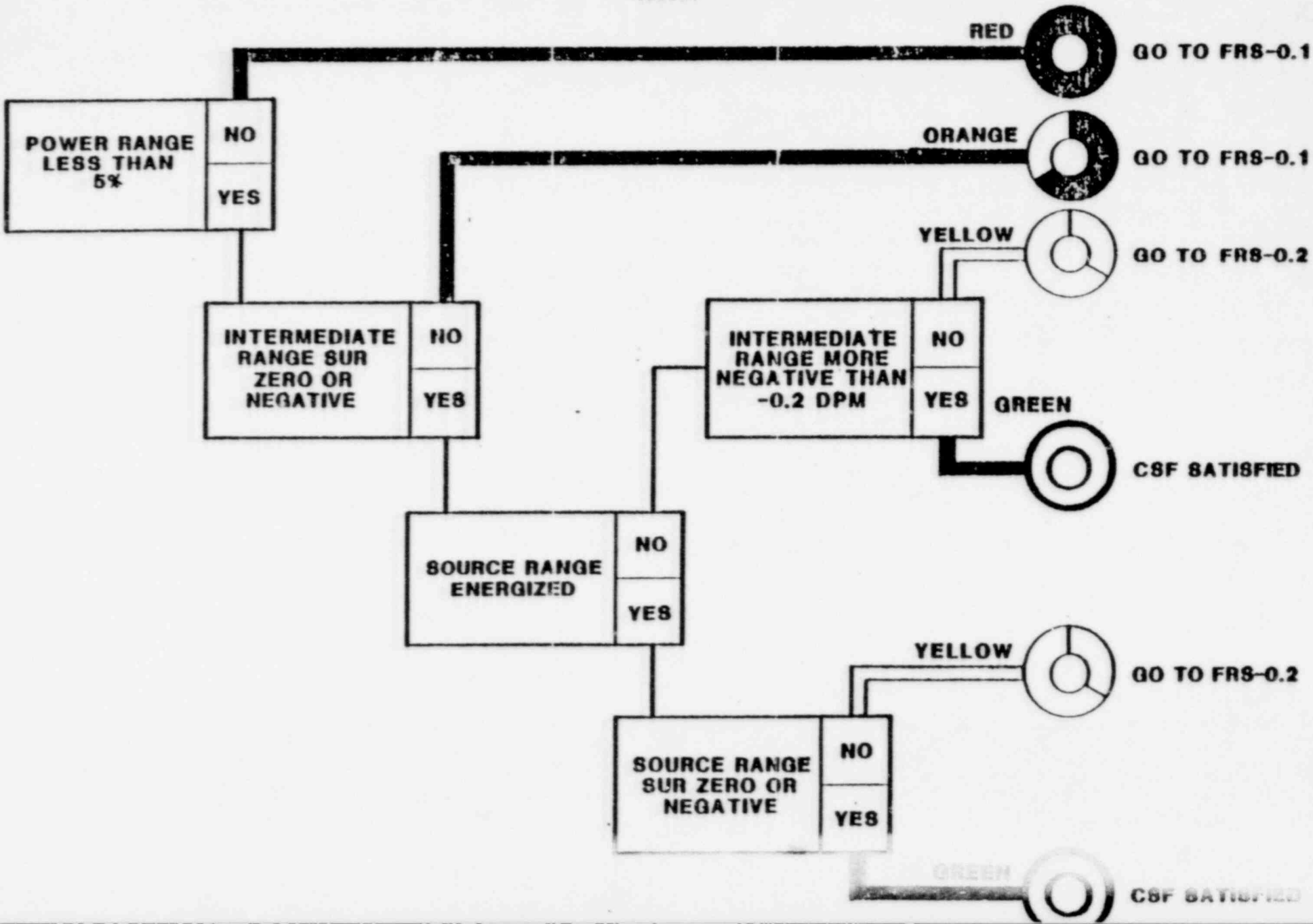
- HARDWARE SELECTION REPORT
- FUNCTIONAL DESIGN SPECIFICATION
- EVALUATION PROGRESS REPORT
- HUMAN FACTORS GUIDELINES
- TRAINING PROGRAM
- EXPERIENCE SUMMARY REPORT

SPDS PROJECT PERSONNEL INTERFACE WITH PLANT OPERATIONS PERSONNEL



SUBCRITICALITY

Rev.1

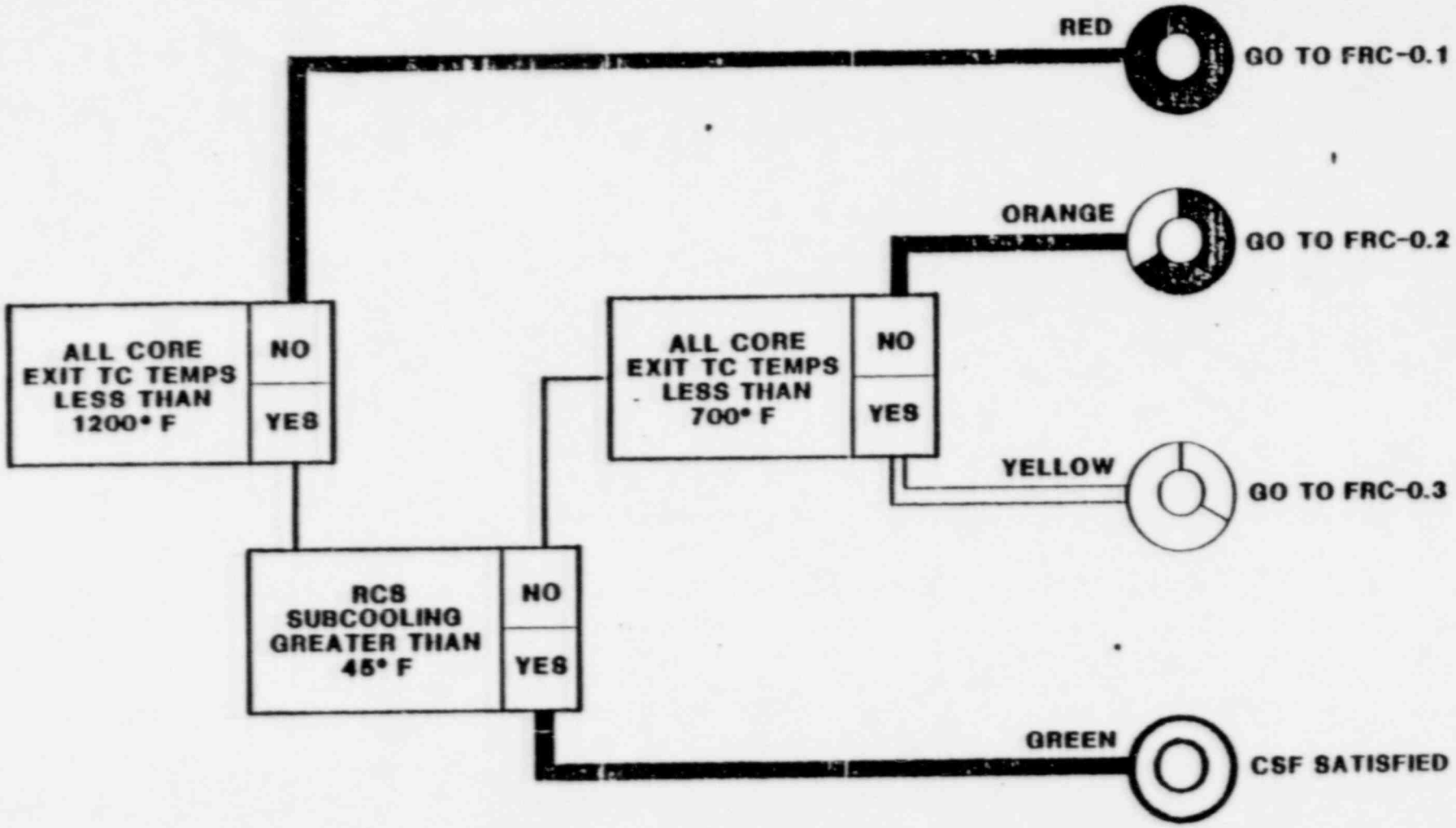


XII-3.28

01-8504

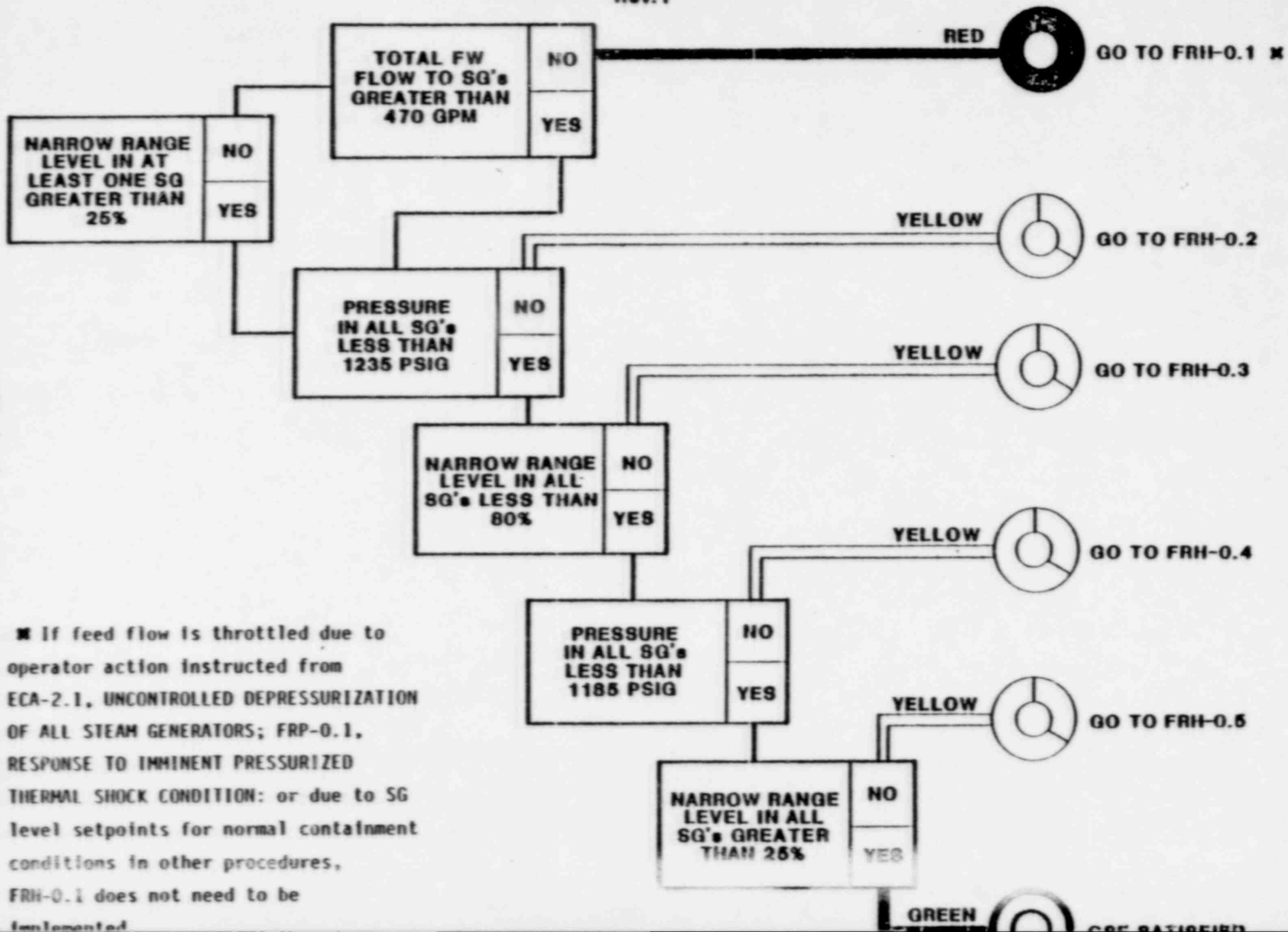
CORE COOLING

Rev. 1



HEAT SINK

Rev.1



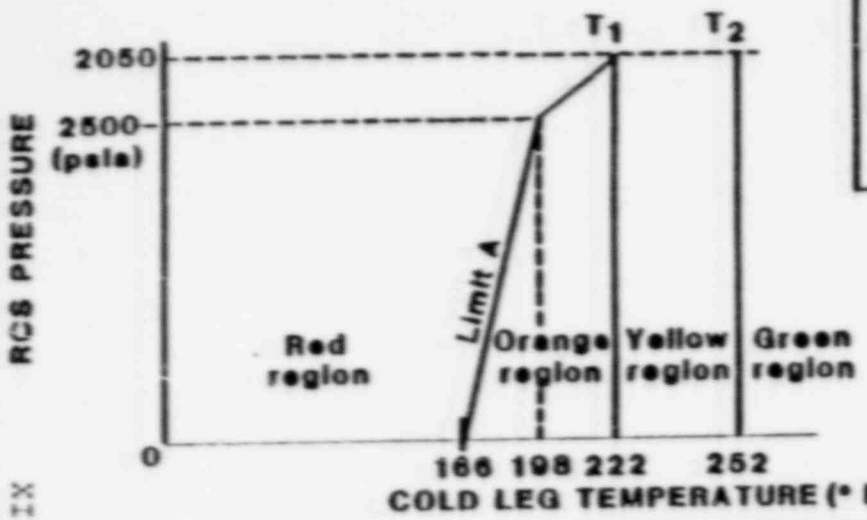
✖ If feed flow is throttled due to operator action instructed from ECA-2.1, UNCONTROLLED DEPRESSURIZATION OF ALL STEAM GENERATORS; FRP-0.1, RESPONSE TO IMMINENT PRESSURIZED THERMAL SHOCK CONDITION: or due to SG level setpoints for normal containment conditions in other procedures, FRH-0.1 does not need to be implemented.

XII-3.30

01-8504

INTEGRITY

Rev. 1



RCS TEMP. (° F)	RCS PRESS. (psig)
70	438
100	438
150	495
200	570
235	815
274	1400
300	2100
313	2450

COLD OVERPRESSURE LIMIT

ALL RCS PRESSURE-COLD LEG TEMPERATURE POINTS TO RIGHT OF LIMIT A — NO → RED → GO TO FRP-0.1; YES

ALL RCS COLD LEG TEMPERATURE GREATER THAN 222° F — NO → ORANGE → GO TO FRP-0.1; YES

ALL RCS COLD LEG TEMPERATURE GREATER THAN 252° F — NO → YELLOW → GO TO FRP-0.2; YES → GREEN → CSF SATISFIED

ALL RCS COLD LEG TEMPERATURE GREATER THAN 222° F — NO → ORANGE → GO TO FRP-0.1; YES → YELLOW → GO TO FRP-0.2

RCS PRESSURE LESS THAN COLD OVERPRESSURE LIMIT — NO; YES → GREEN → CSF SATISFIED

TEMPERATURE DECREASE IN ALL COLD LEGS LESS THAN 100° F IN THE LAST 60 MINUTES — NO; YES

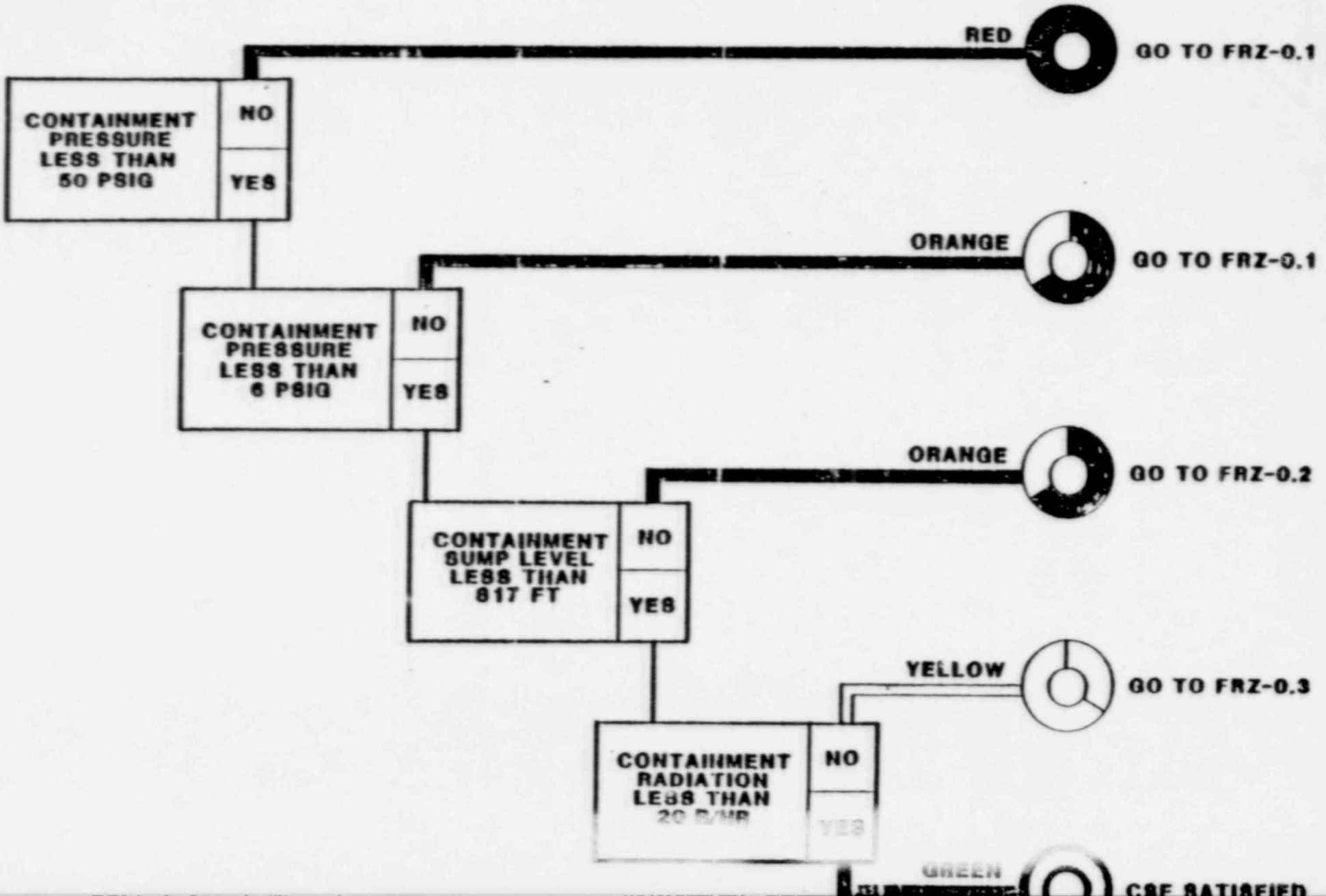
RCS TEMPERATURE GREATER THAN 350° F — NO; YES → GREEN → CSF SATISFIED

XII-3.31

01-8504

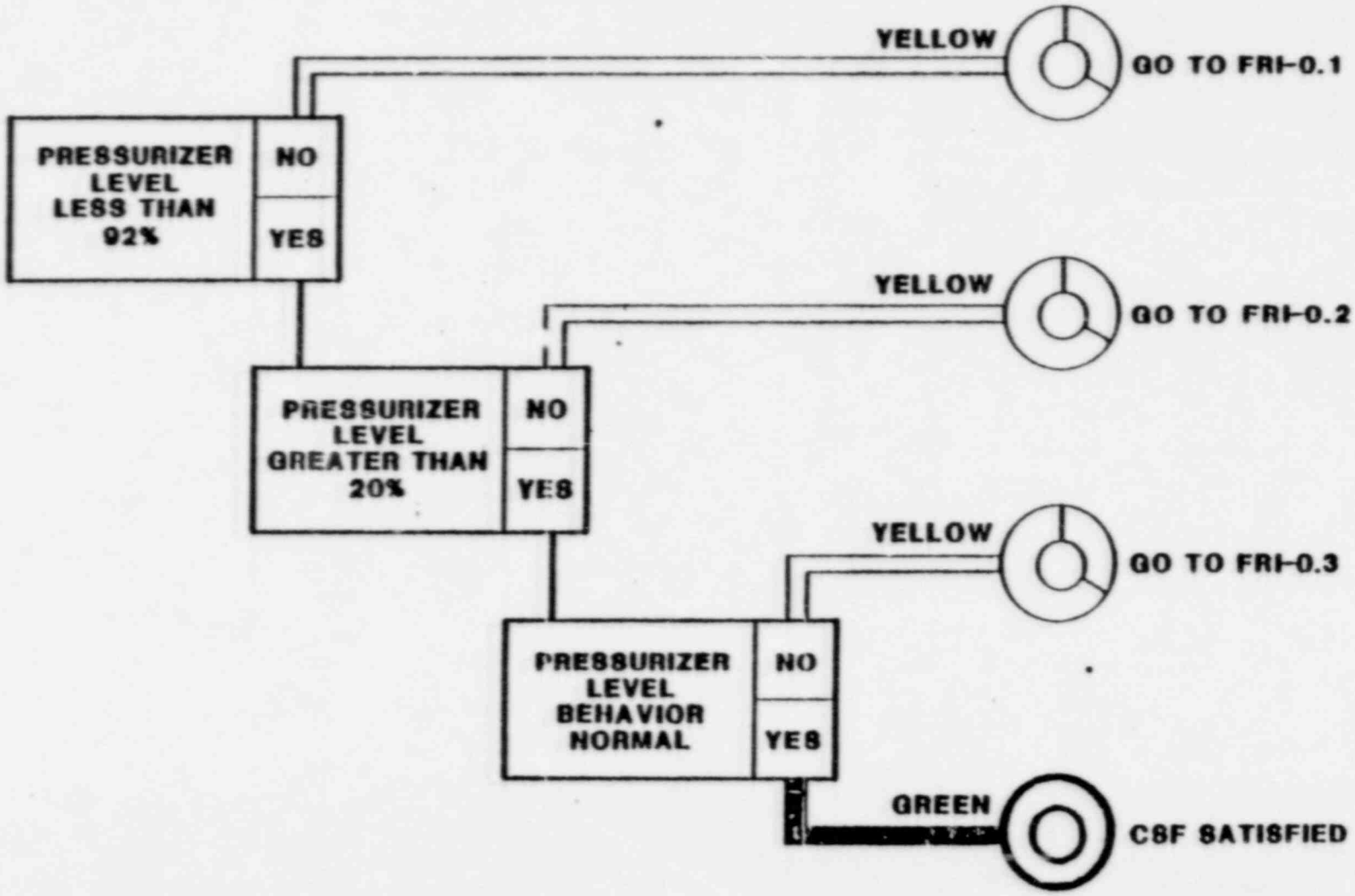
CONTAINMENT

Rev. 1



INVENTORY

Rev. 1



SCENARIO

For

SPDS AUDIT

PRESENTED TO
THE NRC AUDIT TEAM
JUNE 26, 1985

BY
NORMAN TERREL
TEXAS UTILITIES GENERATING COMPANY

DISCUSSIONS

1) Operations Department Philosophy On SPDS.

2) How Does STA Begin Monitoring
The Critical Safety Function Status Trees ?

3) Scenario

OPERATIONS PHILOSOPHY ON SPDS

SPDS displays are used as aids in evaluating plant parameters and possible trends that may be occurring to which the operators may need to give immediate special attention during any accident condition. It also provides the primary means of continuously evaluating the Critical Safety Functions during any accident condition.

For the entire set of trees, priority of operator action is given by the following:

1) REDs (Extreme challenges), in tree order
2) ORANGEs (Severe challenges), in tree order
3) YELLOWs (Not Satisfied), in tree order

As an example, a RED condition for Core Cooling is of higher priority than a RED condition for Containment (order of trees). However, the RED condition for Containment is of higher priority than any ORANGE condition (order of colors).

2.3 Status Trees Usage

The predefined and prioritized Status Trees provide the mechanism that coordinates event-related recovery and function-related restoration. The Emergency Response Guideline "rules of usage" require the operator to start Status Tree monitoring when the symptoms of the emergency transient result in transition out of guideline E-0, REACTOR TRIP OR SAFETY INJECTION, or when so instructed in guideline E-0. Since a transition out of E-0 is expected during the event-related diagnosis, the Critical Safety Function Status Trees are monitored soon after the reactor trip or safety injection. However, if the operator does not make a transition out of E-0 due to lack of appropriate symptoms, E-0 gives explicit instruction to monitor the Status Trees while remaining in E-0. Placement of this instruction after the verification of automatic actions and the diagnostic sequence is due to various reasons. Verification of automatic actions ensures that plant equipment is operating properly. These steps are performed prior to monitoring the Status Trees since the proper operation of the safeguards equipment is the first means of preventing or correcting any challenges to the Critical Safety Functions. The diagnostic sequence can be performed fairly quickly and any transition to another Optimal Recovery Guideline would require that the Critical Safety Function Status Trees be monitored. Hence, the step to explicitly monitor the Status Trees in E-0 follows these actions. In addition, any extreme challenges to the Critical Safety Functions due to equipment failure are addressed by explicit transitions out of the immediate action steps in E-0.

STEP	ACTION/EXPECTED RESPONSE	RESPONSE NOT OBTAINED
13	Check If SGs Are Not Faulted:	
	a. Check pressures in all SGs - • NO SG PRESSURE DECREASING IN AN UNCONTROLLED MANNER • NO SG COMPLETELY DEPRESSURIZED	a. Go to EOP-2.0, FAULTED STEAM GENERATOR ISOLATION, Step 1.
14	Check If SG Tubes Are Not Ruptured: • CEV pump radiation - NORMAL • SG blowdown radiation - NORMAL • Main steamline radiation - NORMAL	Go to EOP-3.0, STEAM GENERATOR TUBE RUPTURE, Step 1.
15	Check If RCS Is Intact: • Containment radiation - NORMAL • Containment pressure - LESS THAN 3.0 PSIG • Containment recirculation sump levels - NORMAL	Go to EOP-1.0, LOSS OF REACTOR OR SECONDARY COOLANT, Step 1.

STEP	ACTION/EXPECTED RESPONSE	RESPONSE NOT OBTAINED
16	Check If ECCS Flow Should Be Reduced:	
	a. RCS subcooling - GREATER THAN 15°F	a. DO NOT STOP ECCS PUMPS. Go to Step 18.
	b. Secondary heat sink: • Total AFW flow to SGs - GREATER THAN 470 GPM -OR- • Narrow range level in at least one SG - GREATER THAN 10%	b. IF neither condition satisfied, THEN DO NOT STOP ECCS PUMPS. Go to Step 18.
	c. RCS pressure - STABLE OR INCREASING	c. DO NOT STOP ECCS PUMPS. Go to Step 18.
	d. PRZR level - GREATER THAN 20%	d. DO NOT STOP ECCS PUMPS. Try to stabilize RCS pressure with normal PRZR spray. Return to Step 16a.
17	Go to EOS-1.1, SI TERMINATION, Step 1.	
18	Initiate Monitoring Of Critical Safety Function Status Trees.	

SCENARIO

Feedline Rupture Followed By A Steam Generator Tube Rupture.

- Actual Scenario Time Is 7 Hours.
- Demonstration Will Be From 30 To 60 Minutes.

INITIAL CONDITIONS

1) Centrifugal Charging Pump TRAIN A
   Out For Maintenance

2) Motor Driven Auxiliary Feedwater Pump TRAIN A
   Out For Maintenance.

3) Unit is at 100% Power.

4) All Plant Parameters Are Stable.

5) All Unit 2 Systems Are Out Of Service.

EMERGENCY PROCEDURES USED

1. EOP-0.0	Reactor Trip Or Safety Injection.
2. EOP-2.0	Faulted Steam Generator Isolation .
3. EOP-1.0	Loss Of Reactor Or Secondary Coolant
4. EOS-1.3	Transfer To Cold Leg Recirculation
5. EOP-3.0	Steam Generator Tube Rupture.
6. ECA-3.1	SGTR With Loss Of Reactor Coolant - Subcooled Recovery Desired.
7. FRZ-0.1	Response To High Containment Pressure.
8. FRH-0.5	Response To Low Steam Generator Level.
9. FRI-0.2	Response To Low Pressurizer Level.
10. FRC-0.1	Response to To Inadequate Core Cooling.

These are entered from the
Critical Safety Function Status Trees.

FRZ-0.1

FRH-0.5

FRI- 0.2

FRC- 0.1

SCENARIO

Initiating Event	Indication
1. Feedline Rupture	* Steam Generator No. 4 Pressure Rapidly Decreases. * Containment Pressure Increases. * Containment Water Level Increases. * Phase A and B Isolation. * Steam Generator No. 4 Level Rapidly Decreases.

SCENARIO

Initiating Event	Indication
2. Turbine Driven Auxiliary Feedwater Pump Trips	* Steam Generator 1 & 2 Levels Decrease. * Auxiliary Feedwater Flow Decreases. (Only One Pump Available.)

SCENARIO

Initiating Event	Indication
3. Steam Generator Tube Rupture.	* Pressurizer Level Decreases. * Pressurizer Pressure Decreases. * Core Exit Thermocouple Temperature Increases. * Subcooling Decreases . * Secondary Radiation Increases.

Kyle Davis –

1) Act as Reactor Operator.

2) Follow flow path through procedures.

Russell Smith –

1) Act as STA .

2) Follow SPDS display as required, to aid in determining plant conditions.

Norman Terrel –

Will alert the STA when different Critical Safety Function Status Trees are being challenged.

cc:
Nicholas S. Reynolds, Esq.
Bishop, Liberman, Cook,
Purcell & Reynolds
1200 Seventeenth Street, NW
Washington, D.C. 20036

Robert A. Wooldridge, Esq.
Worsham, Forsythe, Sampels &
Wooldridge
2001 Bryan Tower, Suite 2500
Dallas, Texas 75201

Mr. Homer C. Schmidt
Manager - Nuclear Services
Texas Utilities Generating Company
Skyway Tower
400 North Olive Street, L.B. 81
Dallas, Texas 75201

Mr. Robert E. Ballard, Jr.
Director of Projects
Gibbs and Hill, Inc.
11 Pen Plaza
New York, New York 10001

Mr. A. T. Parker
Westinghouse Electric Corporation
P. O. Box 355
Pittsburgh, Pennsylvania 15230

Renea Hicks, Esq.
Assistant Attorney General
Environmental Protection Division
P. O. Box 12548, Capitol Station
Austin, Texas 78711

Mrs. Juanita Ellis, President
Citizens Association for Sound Energy
1426 South Polk
Dallas, Texas 75224

Ms. Nancy H. Williams
CYGNA
101 California Street
San Francisco, California 94111

Resident Inspector/Comanche Peak
Nuclear Power Station
c/o U.S. Nuclear Regulatory Commission
P. O. Box 38
Glen Rose, Texas 76043

Regional Administrator, Region IV
U.S. Nuclear Regulatory Commission
611 Ryan Plaza Drive, Suite 1000
Arlington, Texas 76011

Larry A. Sinkin
3022 Porter Street, NW #304
Washington, D.C. 20008

Ms. Billie Pirner Garde
Citizens Clinic Director
Government Accountability Project
1901 Que Street, NW
Washington, D.C. 20009

David R. Pigott, Esq.
Orrick, Herrington & Sutcliffe
600 Montgomery Street
San Francisco, California 94111

Anthony Z. Roisman, Esq.
Trial Lawyers for Public Justice
2000 P. Street, NW
Suite 611
Washington, D.C. 20036

Nancy E. Wiegers
Spiegel & McDiarmed
1350 New York Avenue, NW
Washington, D.C. 20005-4798

cc:
Resident Inspector - Comanche Peak
c/o U.S. Nuclear Regulatory Commission
P. O. Box 1029
Granbury, Texas 76048

Mr. John W. Beck
Manager - Licensing
Texas Utilities Electric Company
Skyway Tower
400 N. Olive Street, LB#81
Dallas, Texas 75201

Mr. Jack Redding
Licensing
Texas Utilities Generating Company
4901 Fairmont Avenue
Bethesda, Maryland 20814

William A. Burchette, Esq.
Heron, Burchette, Ruckert & Rothwell
Suite 700
1025 Thomas Jefferson Street, NW
Washington, D.C. 20007

Mr. James McGaughy
Southern Engineering Company of Georgia
1800 Peachtree, Street, NW
Atlanta, Georgia 30367-8301

AUG 13 1985

MEETING SUMMARY DISTRIBUTION

Docket File
NRC PDR
L PDR
NSIC
PRC System
LB#1 Reading File
Project Manager S. B. Burwell
M. Rushbrook
Attorney, OELD
R. Hartfield*
OPA*

NRC Participants

OTHERS
G. Lapinsky
J. Joyce
F. Orr
W. Regan

bcc: Applicant & Service List

*Caseload Forecast Panel Visits