NUREG/CR-1999

Human Engineering Guidelines for Use in Preparing Emergency Operating Procedures for Nuclear Power Plants

Manuscript Completed: March 1981
Date Published: April 1981

Prepared by
F. Fuchs, J. Engelschall, G. Imlay

Xyzyx Information Corporation
21116 Vanowen Street
Canoga Park, CA 91303

Prepared for
Division of Human Factors Safety
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
NRC FIN B6872

ABSTRACT

This report presents recommendations aimed at improving the usability of emergency procedures used in nuclear power plants. The recommendations are based on established presentation principles and a review of typical deficiencies in current nuclear power plant emergency procedures. In support of the recommendations, a summary of these deficiencies and a discussion of the kinds of operator errors affected by procedures are included. The major recommendations are as follows:

1. Adopt a dual-level procedure design.

2. Require a written specification governing procedure design.

3. Employ human factors provisions in the design specification.

4. Require a written specification governing the procedure development process.

5. Continue to make maximum use of the analytical methods now employed.

6. Provide a means to help the plants comply with the specifications.

A model procedure is included to illustrate how these recommendations can be implemented. With regard to the third recommendation, a listing is offered of the kinds of provisions that should be employed.

CONTENTS

LIST OF TABLES AND FIGURES

PREFACE

This report documents the second of two tasks performed for the NRC (under contract No. NRC-03-80-118) relative to emergency operating procedures for nuclear power plants. The aim of the project was to improve the quality of such procedures through the application of human factors principles. The primary focus of attention is on a particular subset of emergency procedures pertinent to small-break loss-of-coolant accidents (LOCA).

In the first task, emergency procedures from nine nuclear power plants were evaluated for usability. The investigation included visits to several plants and their simulators. Recommendations for improving the procedures were made on a plant-by-plant basis. The results of that effort are summarized in a separate document, Evaluation of Emergency Operating Procedures for Nuclear Power Plants (NUREG/CR-1875).

In the second task, emergency procedures were examined from a more global viewpoint. This latter examination included considerations of the development process, the circumstances of use, and the state of the art relative to procedure design. Recommendations were then formulated for NRC use in behalf of the entire industry.

This report is presented in three sections. In Section 1, operator errors are analyzed for the purpose of showing how they can be affected by written procedures. In Section 2, an assessment is made of the emergency procedures from nine nuclear power plants. Deficiencies are examined in terms of the kinds of errors they could invite. In Section 3, recommendations are made on behalf of improved procedures throughout the industry. The recommendations include a model emergency procedure. Appendix A has been included to show parallel developments in emergency procedures from other industries.

SECTION 1

OPERATING PROCEDURES AND WORK ERRORS

There is general agreement that operator errors can cause and aggravate system failure in the nuclear power industry. In the Finnegan study (Ref. 1 and 2), it was estimated that between 20% and 25% of power plant failures were a result of human error. The authors called this a conservative estimate. Merrill Taylor of the NRC (Ref. 3), informed the Lewis Committee in 1978 that from 50% to 85% of the hypothetical safety system failures he examined would be caused by human error. Another analysis of Licensee Event Reports (LERs) determined that 20% to 50% of LER failures are attributable to human error (Ref. 4). No matter which set of figures is cited, the problem of human error is obviously too large to be ignored.

As the nuclear industry looks for ways to control human error, an increased amount of attention is being given to defining and measuring it. The work of Swain and Guttman (Ref. 3) provides a good example of this new direction. To date, however, there has been no study within the industry of the connection between specific kinds of errors and operating procedures.

In the present report, error definition is taken up with that objective in mind. Operator errors are analyzed for the purpose of showing how they can be affected by written procedures. The approach used was derived from the work of Inaba in the Air Force study, Presentation of Information for Maintenance and Operations (PIMO). Inaba found that maintenance errors could be reduced to nearly zero by the application of human factors principles to the procedures (Ref. 5).

Among the principles developed in the PIMO project are rules regulating sentence structure and sentence length, nomenclature control, verb control, and a standard, concise format. Sentence structure, for example, is kept short, so that a minimum of interpretation is required. The standard syntax is a command verb followed by a direct object.

Because the application of human factors principles to procedures is a generic problem of information transfer, these principles can and have been applied to maintenance, operations, and administraive procedures.

In this section, the principles established for maintenance procedures in the PIMO Project are applied to operating procedures in nuclear power plants. The analysis that follows is further supported by the plant observations made in Task I, evidence provided in Swain and Guttman (Ref. 3) and Seminara, Gonzalez, and Parsons (Ref. 6), and extensive personal experience in procedural technology. The discussion is presented under these headings:

- Work Conditions and Job Duties
- Kinds of Errors Made by Operators
- General Causes of Operator Errors
- Specific Causes of Operator Errors
- Reduction of Operator Errors

1.1 WORK CONDITIONS AND JOB DUTIES

The kinds of errors made by nuclear power plant operators in connection with emergency procedures are influenced by the conditions under which operators work and the duties they are expected to perform.

1.1.1 Work Conditions

The job of concern is that of responding to emergencies such as a small-break loss-of-coolant accident (LOCA). The work takes place in a control room manned by several operators. LOCA procedures vary widely in scope and duration. Some are quite long, exceeding 100 steps in length.

The work is characterized by procedure-following, involving the manipulation of controls and the extraction of information from indicators. Demands for quick reaction, superior strength, and/or sensorimotor skills are minimal. Demands for mathematical computation and logical decision making appear at various points in the process.

The operators are licensed based on qualifications derived from three years of training and plant experience. Their training includes practice of emergency situations in dynamic simulators. However, following assignment to a plant, the typical operator seldom receives practice on each emergency procedure more than once each year.

Emergency situations carry serious implications for both plant safety and plant productivity. Emergencies therefore may be accompanied by varying degrees of psychological stress. The stress level associated with a small-break LOCA has been referred to as "moderately high." A moderately high level of stress is one that results in some disruption in the performance of most persons (Ref. 3).

The final descriptor on work conditions concerns system design. Most control rooms are arranged in the form of three large panel boards, augmented by additional controls and indicators located nearby. The controls and indicators used in emergency procedures are not grouped conveniently in one single area. They are distributed across all three panels. In the past year a significant attempt has been made to improve the man-machine interface through the removal of problems such as: poor design and layout of control panels, poor labeling of controls and indicators, inadequate indications of plant status, and presentation of nonessential information. However, such problems still exist in some plants.

1.1.2 Job Duties

Within the environment summarized above, the operator is expected to perform certain duties in response to emergencies. Stated in their simplest terms, these duties fall into three categories:

- Responding to system signals denoting the presence of an emergency
- Executing prescribed courses of action
- Selecting strategies for novel situations

Responding to system signals denoting the presence of an emergency. This duty is keyed to the system design, which employs annunciators to indicate specific plant conditions. The annunciators are responsible for capturing the operator's attention. The operator then relies on his memory to tell him the required reaction in each case. In stipulated emergencies, the required reaction is to obtain the corresponding emergency procedure. The link between annunciator and procedure must be created and reinforced by training.

Executing prescribed courses of action. This duty represents the bulk of the activity experienced by the operator. The nature of the work in nuclear power plants is such that it is nearly always prescribable in advance, at the detail level. Since engineering designs and operating demands tend to remain stable once established, step sequences need not be changed with great frequency. Therefore, prescribed courses of action can be committed to printed form with the expectation that they too will remain stable. Prescribed courses of action in procedural form are especially applicable to emergency situations.

Selecting strategies for novel situations. This duty is intended to be small in scope and continuously shrinking over time. The reason is that novel situations represent risks that each plant wishes to avoid. The way of reducing that risk is to convert novel situations into prescribed courses of action as quickly as possible. The source of each new prescription is the information produced by system analysis. However, analysis is a slow and deliberate process. Until such time as all contingencies are covered by prescribed courses of action, operators must rely on their knowledge of the system, as obtained through training and experience.

1.2 KINDS OF ERRORS MADE BY OPERATORS

Given these work conditions and job duties, all operators are vulnerable to certain kinds of errors. These kinds of errors are summarized in Table 1-1.

TABLE 1-1

KINDS OF WORK ERRORS MADE BY OPERATORS

1. Responding to System Signals Denoting Presence of Emergency a. Fail to detect key signals b. React incorrectly (1) Assume no emergency (2) Go to wrong emergency procedure
2. Executing Prescribed Courses of Action a. Omit steps b. Execute steps in wrong sequence c. Execute steps incorrectly (1) Misread indicator (2) Select incorrect controls (3) Operate controls incorrectly (4) Perform calculations incorrectly (5) Make incorrect decisions
3. Selecting Strategies for Novel Situations a. Make incorrect decisions

When responding to system signals denoting the presence of emergencies, operators may fail to detect the signals, or they may react incorrectly in one of two ways: by assuming that no emergency exists or by going to the wrong emergency procedure.

When executing prescribed courses of action, operators may omit steps, execute steps in the wrong order, or execute steps incorrectly in five different ways: by misreading indicators, selecting incorrect controls, operating controls incorrectly, performing calculations incorrectly, or making incorrect decisions.

When selecting strategies for novel situations, operators may make incorrect decisions. Once they select a particular strategy, of course, they must prescribe a course of action. All subsequent error risk therefore reverts to that category.

1.3 GENERAL CAUSES OF OPERATOR ERRORS

In the work environment described here, several common causes of work error appear not to apply. Such causes include lack of strength, lack of speed, and lack of sensorimotor skill. The causes that remain occupy only two general categories: lack of information and lack of attention. Lack of information means that the operator is without the proper facts at the precise point of need. Lack of attention means that he has the proper facts but for some reason is not applying them. The two general causes are shown in Table 1-2, in conjuction with the kinds of work error made by the operator.

As indicated in Table 1-2, the two general causes are not distributed evenly across all kinds of errors. For instance, failure to detect key signals (when they are provided) can never be attributed to lack of information. It is caused exclusively by lack of attention. This condition can be aggravated by poor system design, as will be shown later in the discussion. Within the present context, however, it is important to concentrate on factors that can be influenced by the procedures, whether or not the system design is effective.

Note that in executing prescribed courses of action, nearly all the kinds of errors listed are caused by both lack of information and lack of attention.

Note further that the risk of making incorrect decisions appears in two categories. In each case the problem is attributed solely to lack of information.

TABLE 1-2

GENERAL CAUSES OF OPERATOR ERRORS

KINDS OF ERRORS	GENERAL CAUSES OF ERRORS	
	LACK OF INFORMATION	LACK OF ATTENTION
1. Responding to System Signals Denoting Presence of Emergency		
a. Fail to detect key signals	---	•
b. React incorrectly:		
(1) Assume no emergency	•	---
(2) Go to wrong emergency procedure	•	---
2. Executing Prescribed Courses of Action		
a. Omit steps	•	•
b. Execute steps in wrong sequence	•	•
c. Execute steps incorrectly:		
(1) Misread indicators	•	•
(2) Select incorrect controls	•	•
(3) Operate controls incorrectly	•	•
(4) Perform calculations incorrectly	•	•
(5) Make incorrect decisions	•	---
3. Selecting Strategies for Novel Situations		
a. Make incorrect decisions	•	---

1.4 SPECIFIC CAUSES OF OPERATOR ERRORS

Within the two general causes of operator error, there lie six specific causes. They are:

- Distraction by Other Stimuli
- Ineffectively Expressed in Procedure
- Incorrectly Stored in Memory
- Low Motivation
- Not in Memory
- Not in Procedure

The six specific causes are shown in Table 1-3, in conjunction with the kinds of work errors made by the operator and the two general causes.

The first general cause, lack of information, could result from any of four specific causes, namely:

- Information not in memory (operator forgot or never learned it)

- Information incorrectly stored in memory (operator only thinks he remembers it)

- Information not in procedure (procedure lacks key details)

- Information ineffectively expressed in procedure (procedure hard to use)

The second general cause, lack of attention, on the other hand, arises from two specific causes:

- Operator distracted by other stimuli
- Operator not highly motivated

Note in Table 1-3 that certain error-likely situations may be further aggravated by poor system design. All such cases involve either system outputs or system hardware configurations.

TABLE 1-3

SPECIFIC CAUSES OF OPERATOR ERRORS

KINDS OF ERRORS	SPECIFIC CAUSES OF ERROR	
	LACK OF INFORMATION	LACK OF ATTENTION
1. Responding to System Signals Denoting Presence of Emergency		
a. Fail to detect key signals	--	DI; LM *
b. React incorrectly:		
(1) Assume no emergency	NM	--
(2) Go to wrong emergency procedure	IS	--
2. Executing Prescribed Courses of Action		
a. Omit steps	NM; NP	DI; LM
b. Execute steps in wrong sequence	NM; NP	DI; LM
c. Execute steps incorrectly:		
(1) Misread indicator	IS; IE *	DI; LM
(2) Select incorrect controls	IS; IE; NP *	DI LM
(3) Operate controls incorrectly	IS; IE *	DI LM
(4) Perform calculations incorrectly	IS; IE; NP	DI; LM
(5) Make incorrect decisions	IS; IE; NP	--
3. Selecting Strategies for Novel Situations		
a. Make incorrect decisions	NM; IS	--

KEY TO SPECIFIC-CAUSE ABBREVIATIONS

DI Distraction by other stimuli
IE Ineffectively Expressed in procedure
IS Incorrectly Stored in memory
LM Low Motivation
NM Not in Memory
NP Not in Procedure

* Risk of error may be aggravated by poor system design.

1.5 REDUCTION OF OPERATOR ERRORS

Reduction of errors is discussed under the following headings:

- Errors Due to Lack of Information
- Errors Due to Lack of Attention

1.5.1 Errors Due to Lack of Information

Methods of reducing errors due to lack of information are summarized in Table 1-4 and explained below.

Lack of information affects operator performance when reacting to emergency signals, executing prescribed courses of action, and reacting to novel situations. Procedures can influence one of these three action categories directly and two indirectly.

Direct impact is possible when executing prescribed courses of action. Procedures can fill the void where lack of information leads to omission of steps, performing steps in the wrong order, executing steps incorrectly, and dealing with poorly designed controls and indicators. Such gains are accomplished by providing direction at the step level of detail, designing the procedures for maximum usability, and employing notes and cautions to alert the operator to controls and indicators that do not look or function as he might expect.

Procedures can exert indirect influence on the remaining two categories, where operators react incorrectly to emergency signals and where incorrect decisions are made in novel situations.

Procedure-writing personnel must define the linkage between each emergency signal and its respective emergency procedure. At that point, training can be used to reinforce that linkage until it functions reliably for every operator.

System analysis must be used to identify all contingencies. Then, each contingency can be covered by a procedure, thus reducing the frequency and variety of novel situations.

TABLE 1-4

REDUCTION OF OPERATOR ERRORS DUE TO LACK OF INFORMATION

REACTING TO EMERGENCY SIGNALS (Reacting Incorrectly)
Information Not in Memory, Information Incorrectly Stored in Memory Errors are invited by the operator's unreadiness to deal with emergency signals. Remedy: Have procedure personnel define the linkage between each emergency signal and its respective emergency procedure. Have training personnel reinforce that linkage until it functions reliably for every operator.
EXECUTING PRESCRIBED COURSES OF ACTION (Omitting Steps/Performing Steps in Wrong Order)
Information Not in Memory, Information Not in Procedures Errors are invited by the operator's forgetting key pieces of information and being unable to find them in the procedures. Remedy: Design procedures at the step level of detail.

TABLE 1-4

REDUCTION OF OPERATOR ERRORS DUE TO LACK OF INFORMATION
(Continued)

EXECUTING PRESCRIBED COURSES OF ACTION (Continued) (Executing Steps Incorrectly)
Information Incorrectly Stored in Memory, Information Ineffectively Expressed in Procedures, Information Not in Procedures Errors are invited by the operator's tendency to think he remembers the procedure when in fact he does not. Remedy: Design procedures for maximum usablity, to promote user acceptance and facilitate proper learning. Include "how-to" information. Poor System Design (Controls and Indicators) Errors are invited by indicators and controls that do not look or function as might be expected by the operator. Remedy: Use notes and cautions to alert the operator when he is about to encounter such controls and indicators in the procedure.
REACTING TO NOVEL SITUATIONS (Making Incorrect Decisions)
Information Not in Memory, Information Not in Procedures Errors are invited by the occurrence of situations that have no precedent in the operator's memory or supporting documentation, including system analysis. Remedy: Structure the system analysis in such a way as to identify all contingencies. Extend the procedures to cover those contingencies.

1.5.2 Errors Due to Lack of Attention

Methods of reducing errors due to lack of attention are summarized in Table 1-5 and explained below.

Lack of attention affects operator performance when reacting to emergency signals and when executing prescribed courses of action. It is unlikely to apply when the operator is reacting to a novel situation.

Procedures can influence two of the three specific causes of error shown in the table. The cause they cannot affect is the one involving poor system design. If the annunciators are too weak or improperly located, they might fail to attract operator's attention. In such cases, hardware redesign and/or further training are the only remedies available.

Procedures can definitely reduce the incidence of inattention that leads to the omission of steps, performing steps in the wrong order, and executing steps incorrectly. Two mechanisms are available for this purpose. One is to design the procedures for maximum usability, thus promoting user acceptance (Ref. 5 and 6). The other is to require that all work be checked, preferably by a second operator or supervisor. Requiring that actions be verified has been shown to reduce the probability of error (Ref. 3).

1.6 SUMMARY

Operator errors are caused by a number of factors, ranging from poor hardware design to poor training, poor management, and poor procedures. In the analysis described here, the emphasis has been on those errors which can be affected by procedures, and the interface between procedures and other causal factors.

TABLE 1-5

REDUCTION OF OPERATOR ERRORS DUE TO LACK OF ATTENTION

REACTING TO EMERGENCY SIGNALS (Failing to Detect Signal)
Poor System Design (Emergency Annunciators) Errors are invited by annunciators that fail to attract the operator's attention reliably. Remedy: Provide annunciators that emit signals perceptable to all operators. Provide practice in annunciator detection.
EXECUTING PRESCRIBED COURSES OF ACTION (Omitting Steps/Performing Steps in Wrong Order, Executing Steps Incorrectly)
Operator Distracted by Other Stimuli Errors are invited by the operator's carelessness while executing the procedure. Remedy: Design procedures at the step level of detail. Provide a verification block for each step. Require that the verification be performed by a separate person. Operator Not Highly Motivated Errors are invited by the operator's disinterest in and possible early abandonment of the procedure. Remedy: Design procedures for maximum usability to promote user acceptance. Provide a verification line for each step of the procedure.

SECTION 2

ASSESSMENT OF CURRENT PROCEDURES

In Section 1, the gravity of the problem was established, work conditions and job duties were described, categories of operation errors were defined, and procedural mechanisms for dealing with those errors were identified. Given these circumstances, how effective are the operating procedures currently in use?

This question is answered by reiterating in part the results of the evaluation conducted in Task I. The data are expressed in terms of procedural deficiencies and suggested remedies.

Disclosure of most of these deficiencies w s a direct result of the checklist evaluation conducted for Task I. Others became apparent during the course of the evaluation, although they were not part of the original evaluation plan. The deficiencies fall into three categories: presentation style, level of detail, and administrative control. The most prominent deficiencies (those found to be a problem with 40% or more of the procedures examined) are summarized in Table 2-1.

In this section, each of these major deficiencies is exemplified and/or discussed. The remedies suggested are intended to be illustrative of the <u>kinds</u> of improvements needed. They are not intended to be technically accurate. Where further detail was needed but the data were unavailable, such things as panel nomenclature and indicator values were invented to complete the illustrative examples.

TABLE 2-1

SUMMARY OF PROCEDURAL DEFICIENCIES

PROBLEM	PROPORTION OF NINE PLANTS REVIEWED
PRESENTATION STYLE	
• Multiple-variable decisions poorly presented	78%
• Commands included in cautions and notes	100%
• Cautions not placed immediately before applicable step(s)	100%
• Actions not grouped under task/activity headings	100%
• Extraneous explanatory information included	50%
• Worksheets not provided or inadequate	50%
LEVEL OF DETAIL	
• Actions not expressed at step level	56%
• Specific control positions and indicator values not provided	44%
• Control/indicator nomenclature not consistent with panel	83%
ADMINISTRATIVE CONTROL	
• Final page not clearly identified	65%
• Missing or incomplete provisions for verification	90%

2.1 MULTIPLE-VARIABLE DECISIONS POORLY PRESENTED

Where a decision must be made based on more than two variables, the information is not always organized to support the decision. Sometimes the information is scattered and difficult to locate; at other times, as in the example below, the decision information is buried in a caution or note paragraph.

2.1.1 Example of Deficiency:

4.8.3 Throttle HPSI pump discharge valves and use auxiliary spray, if required, to control pressure. Maintain pressurizer level between 28% and 57%.

CAUTION: If SIAS has occurred, do not throttle or secure HPSI flow, unless at least 50°F subcooling can be maintained in the RCS, cold leg temperature is stable, or decreasing, and there is level indicated in the pressurizer between 28% and 57%.

2.1.2 Suggested Remedy:

1. Maintain 50°F subcooling to the RCS as follows:

   a. Set RCS temperature indicator controllers TIC-456 and TIC-567 to manual mode. Adjust set points to 50°F less than T_{sat} as indicated by graph in Figure 1.

   b. Monitor TIC-456 and TIC-567 for one minute. See if 50°F subcooling can be maintained.

      If 50°F subc oling cannot be maintained, go to Step 6, below.

      If 50°F subcooling can be maintained, continue.

2. Monitor cold leg temperature recorders TR-123 and TR-234. See if temperature is increasing.

   If temperature is increasing, go to Step 6, below.

   If not, continue.

3. Monitor pressurizer level indicators LI-321 and LI-123. See if readings are between 28% and 57%.

   If readings are <u>not</u> as specified, go to Step 6, below.

   If readings <u>are</u> as specified, continue.

4. Adjust HPSI pump discharge valves HV-1234 and HV-2345 to maintain PI-678 and PI-789 between 456 psig and 567 psig.

   If pressure can be maintained as specified, go to Step 6, below.

   If not, continue.

5. Initiate auxiliary spray by setting the following valves to OPEN:

ASV-654	ASV-432
ASV-543	ASV-321

The salient feature of this remedy is that the user is routed past steps that are not applicable given the particular situation. Another method of presenting multiple-variable decisions is to tabularize the decision criteria. An example of such a table is presented below.

1. Using appropriate temperature recorders (see table), determine hot leg and cold leg temperature trends. Go to step indicated by table.

COLD LEG TREND (TR-0115)	HOT LEG TREND (TR-0111)		
	$\geq$567°F OR INCREASING	$<$567°F AND DECREASING	$<$567°F AND STABLE
$\geq$456°F OR INCREASING	Go to EP-2	Go to EP-2	Go to EP-6
$<$456°F AND DECREASING	Go to EP-2	Go to EP-8	Go to Step 5, Page 3
$<$456°F AND STABLE	Go to EP-4	Go to Step 22, Page 8	Continue

2.2 COMMANDS INCLUDED IN CAUTIONS AND NOTES

Cautions and notes should never be used to deliver command data. Any intended action or decision must carry its own statement number to attract the operator's attention. The example shown below violates this rule.

2.2.1 Example of Deficiency:

NOTE: If RCP motor amps are less than 600 amps or are decreasing with time, an approach to inadequate core cooling is indicated. Take action to increase heat removal from the reactor coolant system and increase reactor coolant inventory if required.

In this example, not only is the command to act buried in a note, but the operator is not told precisely what actions must be taken. A suggested remedy for both of these deficiencies is illustrated below.

2.2.2 Suggested Remedy:

1. Monitor RCP motor ammeter AI-987 for five minutes.

   If reading is greater than 600 amps and not decreasing, go to Step 12, Page 4.

   If reading is less than 600 amps or decreasing, continue.

2. Start residual heat removal pumps RHR-1A and RHR-1B.

3. Start emergency core cooling pumps ECC-123 and ECC-234.

2.3 CAUTIONS NOT PLACED IMMEDIATELY BEFORE APPLICABLE STEP(S)

Cautions and notes should be placed immediately ahead of the steps to which they apply. Any other location incurs the risk of their being read too early or too late for most effective use. An example of a misplaced caution is shown below.

2.3.1 Example of Deficiency

5.11 On receipt of the RWST low level alarm (150,000 gal), RESET the SAFETY INJECTION and CTMT PHASE A ISOLATION signals. Verify that CTMT sump level has increased. Initiate COLD LEG RECIRCULATION as follows:

CAUTION

Do not reset the Safety Injection signals on the containment sump to RHR valves or the diesel generator sequencers.

2.3.2 Suggested Remedy:

The remedy for misplaced cautions is generally quite simple: place the caution immediately before the applicable step. In the example cited above, the remedy is more complex because the operator must continue with the procedure while waiting for the alarm to sound.

NOTE

If RWST LOW LEVEL alarm comes on while performing Steps 6 through 18, note step being performed, then immediately go to Step 19. Be sure to read caution before Step 19.

6. Monitor . . .

18. Set . . .

CAUTION

Do not perform the following step until RWST LOW LEVEL alarm comes on. Reset ONLY the specified signals. DO NOT reset the safety injection signals on the containment sump to RHR valves or the diesel generator sequencers. If Steps 6 through 18 have been performed and RWST LOW LEVEL alarm has not come on, go to Step 20.

19. Reset SAFETY INJECTION and CTMT PHASE A ISOLATION SIGNALS.

    If all Steps 6 through 18 have been performed, go to Step 20, below.

    If not, return to step noted when alarm came on.

Often, as in examples cited earlier, the caution should have been presented as a command step in the first place. In such cases, the remedy is the same as that cited under Heading 2.2.

2.4 ACTIONS NOT GROUPED UNDER TASK/ACTIVITY HEADINGS

Failure to group actions under higher-level headings makes it difficult for the operator to track his actions and keep in mind his overall objectives. An example of this deficiency is shown below.

2.4.1 Example of Deficiency:

3.3 Notify HP to sample containment atmosphere and S/Gs to identify presence of abnormal radioactivity.

3.4 Identify the faulted steam generator by one or more of the following methods:

- 3.4.1 An unexpected rise in the S/G water level with auxiliary feedwater flow reduced or stopped.
- 3.4.2 High radiation from the S/G blowdown line radiation monitor via EMF-34.
- 3.4.3 High radiation from any S/G, as determined by analysis or a sample.
- 3.4.4 Steam Flow/CF Flow mismatch on affected S/G.

3.5 Reset CA modulating valves and secure CA flow to faulted S/G.

- 3.5.1 Monitor CA Condensate Storage Tank level and Upper Surge Tank. CA suction will auto-swap to RN at 2.0 psig suction pressure.
- 3.5.2 Reset Turbine Driven CA pump.

3.6 Close the isolation valve in the steam line to the Turbine CA pump associated with the faulted S/G. If the faulted S/G is "B", unlock and close 1SA-2 (Main Steam 1B to Aux. FDWPT No. 1 Maintenance Isolation). If the faulted S/G is "C", unlock and close 1SA-1 (Main Steam 1C to Aux. FDWPT No. 1 Maintenance Isolation).

3.9 Verify the affected S/G SM PORV is closed by observing decrease in S/G Steam Flow and Status indication on MCB.

2.4.2 Suggested Remedy:

Identify Faulty Steam Generator

1. Request that HP analyze samples of containment atmosphere and blowdown water from each steam generator for presence of abnormal radioactivity.

   If results of sample analysis are not immediately available, go to Step 2, below.

   If results of sample analysis identify faulty steam generator, go to Isolate Faulty Steam Generator, next page.

Identify Faulty Steam Generator (conti..ued)

2. Using Table 1, determine difference in cubic feet per minute (cfm) between steam flow and feedwater flow for each steam generat... .

TABLE 1

STEAM GENERATOR:		A	B	C	D
INSTRU-MENTS	STEAM FLOW:	FIC-1A	FIC-1B	FIC-1C	FIC-1D
	FEED-WATER FLOW:	FIC-2A	FIC-2B	FIC-2C	FIC-2D
READ-INGS	STEAM FLOW:	___cfm	___cfm	___cfm	___cfm
	FEED-WATER FLOW:	- ___cfm	- ___cfm	- ___cfm	- ___cfm
DIFFERENCE IN POUNDS PER HOUR:		= ___cfm	= ___cfm	= ___cfm	= ___cfm

If any difference is greater than +123 cfm, associated steam generator is faulty. Go to Isolate Faulty Steam Generator, next page.

If differences for all steam generators are not greater than +123 cfm, continue.

3. Set auxiliary feedwater flow indicator controllers FIC-123 and FIC-234 to MANUAL mode. Adjust set points to 0. Monitor for readings to start to decrease.

Identify Faulty Steam Generator (continued)

4. Using Table 2, monitor water level of each steam generator for readings to start to decrease.

TABLE 2

STEAM GENERATOR	LEVEL RECORDER
A	LR-45-A
B	LR-45-B
C	LR-45-C
D	LR-45-D

If any water level reading does not decrease, associated steam generator is faulty. Go to Isolate Faulty Steam Generator, below.

If all water level readings decrease normally, tube leak flow is too low to detect by level or flow comparison. Perform EP-1234, Cool Reactor to 507°F, while waiting for results of sample analysis.

Isolate Faulty Steam Generator

1. Using Table 1, stop auxiliary feedwater flow to faulty steam generator by setting appropriate flow indicator controller to MANUAL mode and adjusting set point to 0.

TABLE 1

STEAM GENERATOR	FLOW INDICATOR CONTROLLER
A	FIC-123-A
B	FIC-234-B
C	FIC-345-C
D	FIC-456-D

2. Using Table 1 above, restore normal flow to all non-faulty steam generators by setting appropriate flow indicator controllers to AUTO mode.

Isolate Faulty Steam Generator (continued)

3. Monitor auxiliary feedwater suction pressure indicator PI-987. Verify automatic transfer to nuclear service water when suction pressure reaches 2.0 psig.

4. Reset turbine-driven auxiliary feedwater pump by setting the following switches to AUTO:

CAP-234	CAP-345
CAP-456	CAP-567
CAP-678	CAP-789

5. Using Table 2, set isolation valve associated with faulty steam generator to CLOSE.

TABLE 2

STEAM GENERATOR	ISOLATION VALVE
A	IV-23-A
B	IV-23-B
C	IV-23-C
D	IV-23-D

If faulty steam generator is A or D, go to Step 8, below.

If faulty steam generator is C, unlock 1SA-1 and set to CLOSE. Then go to Step 8.

If faulty steam generator is B, unlock 1SA-2 and set to CLOSE. Continue.

Isolate Faulty Steam Generator (continued)

8. Verify closed status of main steam PORV associated with faulty steam generator as follows:

   a. Using Table 3, monitor steam flow indicator associated with faulty steam generator for reading to decrease.

TABLE 3

STEAM GENERATOR	STEAM FLOW INDICATOR
A	FI-45-A
B	FI-45-B
C	FI-45-C
D	FI-45-D

   b. Using Table 4, monitor status indicator of appropriate PORV on main control board.

TABLE 4

STEAM GENERATOR	STATUS INDICATOR
A	PORV-A
B	PORV-B
C	PORV-C
D	PORV-D

2.5 EXTRANEOUS EXPLANATORY INFORMATION INCLUDED

In several of the procedures evaluated, extraneous explanatory information is included in the procedures. Sometimes this information is included in steps; at other times it takes the form of excessive cautions and notes.

Citing this as a deficiency is not intended to question the value of such information. Explanatory information serves to motivate the operator and, most importantly, help him understand what is happening.

However, such information belongs in training, not in an emergency procedure. In an emergency, the operator needs to know <u>what to do and how to do it</u>. If he's faced with an unforeseen situation, it is too late for him to learn how the system works and why certain actions must be taken. Such information should be carried by system explanation manuals to be used in the operator training program.

An example of extraneous information included in an emergency procedure is shown below.

2.5.1 <u>Example of Deficiency</u>:

.5 Following a period of approximately constant temperature, the primary coolant temperatures increase to well above the secondary saturation temperature, indicating the loss of the heat sink by dryout. This is an important indication of the approach to inadequate core cooling. If the RCP's are off, cold leg temperature will initially increase faster than hot leg temperature, resulting in decreased core ΔT. Use TR-0115 and TR-0125 for cold leg temperatures and TR-0111 and TR-0121 for hot leg temperatures. Using the recorders will show a trend for easier determination of temperature trends.

The remedy for this deficiency is to provide the operator with the information he needs to respond to the emergency. That is, <u>what to do and how to do it.</u> Such information is illustrated on the following page.

2.5.2 Suggested Remedy:

1. Using appropriate temperature recorders (see table), determine hot leg and cold leg temperature trends. Go to step indicated by table.

COLD LEG TREND (TR-0115)	HOT LEG TREND (TR-0111)		
	$\geq$567°F OR INCREASING	$<$567°F AND DECREASING	$<$567°F AND STABLE
$\geq$456°F OR INCREASING	Go to EP-2	Go to EP-2	Go to EP-6
$<$456°F AND DECREASING	Go to EP-2	Go to EP-8	Go to Step 5, Page 3
$<$456°F AND STABLE	Go to EP-4	Go to Step 22, Page 8	Continue

2.6 WORKSHEETS NOT PROVIDED OR INADEQUATE

In an emergency, an operator is sometimes called upon to make computations and record data. Rarely are worksheets provided to facilitate such computations. The excerpt below (reiterated from a previous example for reader convenience) illustrates the need for worksheets.

2.6.1 Example of Deficiency:

3.4.4 Steam Flow/CF Flow mismatch on affected S/G.

2.6.2 Suggested Remedy:

2. Using Table 1, determine difference in cubic feet per minute (cfm) between steam flow and feedwater flow for each steam generator.

TABLE 1

STEAM GENERATOR:		A	B	C	D
INSTRUMENTS	STEAM FLOW:	FIC-1A	FIC-1B	FIC-1C	FIC-1D
	FEEDWATER FLOW:	FIC-2A	FIC-2B	FIC-2C	FIC-2D
READINGS	STEAM FLOW:	___ cfm	___ cfm	___ cfm	___ cfm
	FEEDWATER FLOW:	- ___ cfm	- ___ cfm	- ___ cfm	- ___ cfm
DIFFERENCE IN POUNDS PER HOUR:		= ___ cfm	= ___ cfm	= ___ cfm	= ___ cfm

2.7 ACTIONS NOT EXPRESSED AT THE STEP LEVEL

In the majority of the procedures evaluated, actions were not always expressed as command verbs against specific controls and indicators. An example of this deficiency is presented below.

2.7.1 Example of Deficiency:

a. As the water level (PAMS) in the refueling water storage tank decreases under the action of the safeguards pumps, check that the recirculation sump water level instrumentation indicates an increase in water level in the sump. If a sump water level increase is not evident then a re-evaluation of the symptoms in EOI-0 must be conducted.

2.7.2 Suggested Remedy:

1. Monitor the following refueling water storage tank level recorders and indicators until readings start to decrease:

LR-123	LI-987
LR-234	LI-876
LR-345	LI-765

2. Monitor the following sump water level recorders and indicators for five minutes. See if readings start to increase.

LR-987	LI-123
LR-876	LI-234
LR-765	LI-345

If readings do not increase, re-evaluate the event per EOI-0, Emergency Shutdown.

If readings increase, continue.

2.8 SPECIFIC CONTROL POSITIONS AND INDICATOR VALUES NOT PROVIDED

Although this deficiency occurred in less than half (44%) of the procedures evaluated for Task I, it is included here because of its relative importance. The ambiguity caused by failure to provide specific control positions and indicator valves invites operator errors.

2.8.1 Example of Deficiency:

3. Maintain adequate pressurizer pressure.

2.8.2 Suggested Remedy:

3. Set pressurizer pressure indicator controllers PIC-123 and PIC-234 to MANUAL mode. Adjust set points to 456 psig.

2.9 CONTROL/INDICATOR NOMENCLATURE NOT CONSISTENT WITH PANEL

At five of the six plants visited, the nomenclature used in the procedures was not always identical to that displayed on the controls and indicators. The suggested remedy for this deficiency requires a more rigid procedure development process. The process should include an edit step and/or user test devoted to eliminating these inconsistencies.

2.10 FINAL PAGE NOT CLEARLY IDENTIFIED

Pages are marked for the purpose of assuring the user that he has (or does not have) the complete set. To remedy this deficiency, it is suggested that all pages be marked via the Page ___ of ___ (total) method. Additionally the final page of each procedure should be clearly marked, "Final Page."

2.11 MISSING OR INCOMPLETE PROVISIONS FOR VERIFICATION

Many of the procedures evaluated used no verification scheme whatsoever. Others provided verification lines for some actions, but not all. In an emergency, it is important that all actions be verified by persons other than those performing the actions. This will help negate the effects of inattention.

Verification must be applied to both actions and decisions. Overt actions can be verified by direct observation. Decisions can be verified by requesting that operators articulate the rationale for the decision before performing subsequent actions. Both kinds of verification require administrative action in both planning and implementation. The procedure must provide a basis for the verification by including a sign-off line at each appropriate point.

2.12 SUMMARY

The emergency procedures evaluated for the nine plants involved in the Task I effort have been reviewed here and found to contain clear deficiencies.

In terms of the error analysis described in Section 1, the kinds of deficiencies noted could invite operator errors in executing prescribed courses of action. Such errors would be represented by the omission of steps, the execution of steps in the wrong sequence, and the execution of steps incorrectly. The latter category of error includes:

- Misreading indicators
- Selecting incorrect controls
- Operating controls incorrectly
- Performing calculations incorrectly
- Making incorrect decisions

The cited deficiencies produce a condition of low usability, wherein the risk of operator error may be attributed to both lack of information and lack of attention.

SECTION 3

RECOMMENDATIONS FOR IMPROVEMENT OF EMERGENCY PROCEDURES IN NUCLEAR POWER PLANTS

On the basis of the ideas expressed in Sections 1 and 2, recommendations are advanced for the improvement of emergency procedures in nuclear power plants.

These recommendations are presented under the following headings:

- Emergency Procedure Design
- Emergency Procedure Development Process
- Model Emergency Procedure

3.1 EMERGENCY PROCEDURE DESIGN

The term "design" refers to the physical configuration of the finished procedure. Design factors cover generic concepts such as level of detail, sentence structure, action grouping, nomenclature control, and the use of illustrations. These are mechanisms known to affect the extent to which procedures are understandable, one of the three information properties required by the user.

The recommendations that follow are made in behalf of improved procedure design.

3.1.1 Adopt a Dual-Level Procedure Design

There are two audiences that must be satisfied by the procedures: trainees and licensed operators. Trainees need explicit direction in terms of "how-to" and "where-to" data for every activity they are called upon to perform. Licensed operators typically need only "what-to-do" guidance because they already hold much of the explicit direction in their heads. Thus, it is important that any procedure approach meet the following criteria(Ref. 7):

1. It must be designed for use by the most inexperienced operator.

2. It must aid and not hinder the performance of experienced operators.

3. It must be used in the training of operators.

4. It must be capable of being easily evaluated and monitored by the NRC.

5. It must be acceptable to the operators who use it.

6. It must be acceptable to the utilities responsible for its control.

These criteria are discussed in the paragraphs that follow.

The current approach tries to reach both trainees and licensed operators with the same procedural package. In doing so, it introduces a handicap to each audience. Where a package contains only "what-to-do" guidance (as in some of the procedures evaluated for Task I of this project) and no explicit direction, the licensed operator may be satisfied while the trainee is left without support. Where a package contains both guidance and explicit direction, the trainee is satisfied but the operator is confronted with a great deal of material he already holds in memory. In both situations, the dissatisfied audience tends to lose faith in the procedures.

This is not to say that licensed operators never need explicit direction. Under various conditions, such as long periods without practice, or situations involving high stress, help may be needed in recollecting various details. Moreover, individual operators differ in the extent to which they exhibit this need. The unpredictability of the demand means that the full set of explicit directions must be made available to every operator at all times. None of the procedures examined for Task I were this detailed.

However, it is not necessary to integrate the explicit direction with the guidance instructions. The two could easily be packaged separately and correlated by an indexing scheme. In that way, both operators and trainees would be continuously supported by precisely the kinds of information they need. This dual-level approach is currently used in maintenance procedures developed for the armed forces (Ref. 8).

The aforementioned phrase "faith in the procedures" is a very important factor to consider since such faith (or lack thereof) affects the acceptance of the procedures. If the operators do not accept the procedures, it is highly unlikely that they will use the procedures when needed (Ref. 5).

One factor that promotes user acceptance is the appropriate level of detail. When experienced operators are confronted with unneeded details, exasperation with the procedures is a typical reaction. When trainees are provided with incomplete details, a loss of faith in the procedures results. In both cases, the procedures are not used. It seems clear that both needs cannot be met in a single-level package. A dual-level approach is called for.

When an operator learns a procedure, the details become essentially a sub-routine. At that time, a meaningful title is often a sufficient clue to recall the sub-routine. However, people forget. Thus, easy access to the details is also important.

It is generally accepted that all trainees should use the actual emergency procedures in training(Ref. 7). However, the actual emergency procedures rarely carry sufficient detail to support trainees. The details define the specific behavior required of the operators. If the details are not in the procedure, the trainee must learn them from some other source, e.g., supervisor or peers. Such people are not always reliable sources of information at the step-level of detail.

Besides providing the necessary level of detail for trainees, detailed procedures also give the NRC a method for monitoring the adequacy of procedures and the performance of license candidates. Evaluation of general-level procedures is handicapped by the vague and indefinite actions called for, which indicate objectives or tasks, not precise actions. When precise actions are given, NRC examiners have the data necessary to determine technical accuracy and completeness. This precision also offers the criteria needed by NRC licensing examiners to monitor the performance of trainees or operators who are undergoing qualification examinations.

User acceptance of procedures will satisfy the need of utilities to assure that emergency operations are performed correctly. The detailed procedures will also provide the utilities with relevant and accurate training materials, thereby easing the load on trainers and guaranteeing a clear linkage between classroom and on-the-job training.

The two-package approach should take into account the following provisions:

1. Design one package with less detail for use by the licensed operator. Provide "what" information but not "how to" or "where" information.

2. Design the other package with more detail for use by the trainee. Provide "what," "how to," and "where" information.

3. Let the package with more detail be easily available to the licensed operator when he needs it, (e.g., as an attachment to the less-detailed package) but do not require him to use it when the package with less detail will suffice.

4. Where applicable (due to action complexity or low frequency of occurrence), require that the more-detailed package be followed.

5. Use administrative controls and the operator training program to assure that operators learn to use all procedures properly. Emphasize that the two-package approach gives the operator no license to commit errors if he fails to use the more-detailed procedures when needed.

3.1.2 Require a Written Specification Governing Procedure Design

The advantage of having a set of criteria documented in writing is that it promotes consistency. It settles in advance many of the problems of selecting effective presentation modes. In doing so, it relieves individual writers of having to grapple privately with those same issues and possibly reaching conflicting solutions. A complete specification would include criterion statements and illustrative examples covering all facets of procedure design.

The criterion statements themselves represent the substance of the specifications. Their purpose is to evoke (from the writer) procedures that are understandable to both operators and trainees. That purpose is best met when the criterion statements are based on established principles of information transfer (Ref. 5) rather than the opinions of experts, or common sense, or recent experience, as is so often the case.

Some of these principles are derived from the formal research literature involving perception, information processing, human engineering, and similar technologies. This research has resulted in findings on subjects such as short-term memory; user orientation; consistency and directness of syntax; and format, verb, and nomenclature control -- all of which impact the usability of procedures.

A specification based on such principles already exists and has been used effectively in the nuclear waste disposal industry. Some key provisions of that specification are listed under the heading that follows. They are highly relevant to the present situation. With necessary detail adjustments, the entire specification could be made to serve the nuclear power industry.

3.1.3 Employ Human Factors Provisions in the Design Specification

It has been recommended that a design specification be adopted to govern the packaging and formatting of emergency operating procedures for nuclear power plants.

Such a document would have a number of precedents. The specification mentioned above is currently in use at two nuclear waste disposal sites in Washington and Idaho. Based on the criterion statements contained therein, several hundred operating procedures have been developed and placed into service. The work environments covered by those procedures are highly similar to those faced by nuclear power plant operators.

An entire procedure design specification addresses many topics and encompasses many criterion statements with associated illustrations. It would thus be too extensive to be displayed fully in this report. The purpose here is merely to demonstrate the kinds of criterion statements that would appear in a design specification tailored to the precise needs of the nuclear power industry.

The criterion statements presented here are grouped under the following headings:

- General Provisions
- Less-Detailed Procedure Design
- More-Detailed Procedure Design

3.1.3.1 General Provisions

1. Title the primary emergency procedure so as to be easily linked to an observable emergency condition. Require that the link be reinforced by training.

2. Provide an index in the primary emergency procedure that will lead the user to the proper subsidiary emergency procedure.

3. On the first page of every subsidiary emergency procedure, identify all tasks or activities that must be performed.

4. For each task or activity thus identified, provide, on a separate set of pages, further direction for the user.

5. Make the emergency procedures easily located within the emergency procedure manual.

6. Provide the following identification information on each page:

    - Procedure number and title
    - Date of issue
    - Revision number
    - Page number

7. Mark the final page of the procedure: Page ___ of ___; Final Page.

8. Give the procedure a unique and permanently assigned number.

9. If this is a temporary procedure, clearly mark it with an expiration date.

10. Provide for verification and sign-off of actions by persons other than those performing the actions.

3.1.3.2 Less-Detailed Procedure Design

1. Format the less-detailed procedure as a listing or a diagram or a table.

2. Identify each task or activity to show what must be accomplished. Do not define the steps needed to carry out the task or activity.

3. Arrange the tasks or activities so as to show the sequence in which they must be performed.

4. Where the sequence among particular tasks is of no importance, indicate that sequential control is not necessary.

5. For each task or activity, indicate the first page in the more-detailed procedure where the reader may find further direction.

3.1.3.3 More-Detailed Procedure Design

1. Express the instructions in command statements (steps as opposed to paragraphs). Limit each statement to a maximum of three actions.

2. Assemble related steps under headings denoting the tasks or activities shown in the less-detailed procedure.

3. Arrange the steps so as to show the sequence in which they must be performed.

4. Where the sequence among particular steps is of no importance, indicate that sequential control is not necessary.

5. Where a decision must be made based on more than two variables, organize the information to support the decision.

6. If cautions or notes apply to the performance of specific steps or series of steps, always place them immediately ahead of the step(s) to which they apply.

7. Keep command statements out of cautions and notes.

8. If equipment is operating outside the range specified by the procedure, tell the operator what action(s) to take.

9. Where actions require the use of particular controls, give specific control positions.

10. Where actions require the use of particular indicators, give specific indicator values.

11. Show the panel locations of each control and indicator named.

12. Use nomenclature in the procedure identical to that displayed on the panels, controls, and indicators.

13. Express indicator values called out in the procedure in the same units as are shown on the indicators.

14. If worksheets are needed to facilitate some actions, provide spaces for recording and processing all data.

15. If more than one person is required to perform the procedure, write the procedure to one "primary" user. Make him responsible for coordinating the activity with others.

16. Limit references to external procedures to situations where it would be inconvenient for the operator to have the entire (referenced) instruction reiterated within this procedure.

17. List externally referenced documents at the beginning of each procedure.

3.2 EMERGENCY PROCEDURE DEVELOPMENT PROCESS

The term "development process" refers to the particular steps that must be undertaken to create the procedure. The development process affects all three of the procedural properties required by the user. Its fundamental influence is on completeness and accuracy. However, it also interacts with design, to influence understandability. The following recommendations are made to help improve the development process for emergency operating procedures.

3.2.1 Require a Written Specification Governing the Procedure Development Process

Written development process specifications foster improvement in procedure quality wherever they are applied. That improvement normally appears in terms of increased accuracy, completeness, and understandability.

Such gains are made possible by the fact that, in an organized process, the tasks representing the flow of work are identified, described, and interrelated. Intermediate products become visible as task outputs. Checks can then be devised to detect and correct errors as they occur.

Checking represents a vital series of actions in the process. Checks made by subject matter experts enhance procedure accuracy and completeness. Checks made by editorial personnel enhance procedural understandability through compliance with the design specification. Performance testing by typical users provides further assurance of procedure understandability.

Therefore, it is recommended that the process specification include descriptions of the following:

1. The method used to analyze the system to which the procedures apply.

2. The checks used by subject matter experts to assure the accuracy and completeness of the procedures.

3. The edits used to assure compliance with the procedure design specification.

4. A performance test to assure usability of the procedures.

3.2.2 Continue To Make Maximum Use of the Analytical Methods Now Employed

System analysis is the keystone of the development process. It provides the information base from which the procedures are eventually written. The ultimate source of that information base is the original set of engineering documents defining the system. Such documents are necessary but not sufficient for reference by the writer. Engineering source data describes essentially what should be happening in system operation. When used in the preparation of emergency procedures, they must also be made to disclose what has gone wrong and what actions must be taken by the operator. System analysis extracts such information by concentrating on the relationships among system components in the various modes of operation.

For maximum effectiveness, system analysis must provide for exhaustive coverage of the system, exploration of all interfaces among system components, and complete documentation of analytical results.

Only in this way can a proper basis be formed for the construction of emergency procedures. Without it there can be no assurance that all contingencies have been identified. Where that assurance is lacking, the risk of operator error in non-routine problem situations increases significantly.

Rigorous analytical methods are already in use by the Owners' Groups. However, they are not in all cases fully documented. The analytical methods of the Owners' Groups should be carefully expressed in written form. The Owners' Groups should then continue to apply their methods with the same degree of dedication that they now show.

3.2.3 Provide a Means To Help the Plants Comply with the Specifications

Despite the sound analytical efforts of the Owners' Groups, plant-specific procedures still tend to be highly variable in quality. It is evident that in some plants further help is needed with the writing portion of the development process.

This condition could be alleviated to some degree by the adoption of a design specification as discussed earlier. However, based on experience gained in developing procedures for other industries, a design specification alone will not suffice. A definite process must be employed to give assurance that the specification will be met.

For most dependable results, that process should be expressed in writing and applied consistently across all writers and all procedures. Further, it should take into account the interface between procedures and training. Each specific performance requirement must be allocated to one or the other. Such allocation is best done on a systematic basis.

This prescription views procedure development in the same light as hardware manufacture. Both are dependent on in-process controls, without which design criteria would be ineffectual. Of the two, procedures have the greater need for such controls because procedures nearly always originate in people-dominated situations, and people always introduce variability.

3.3 MODEL EMERGENCY PROCEDURE

A model emergency procedure is presented here for the purpose of exemplifying the recommended design criteria.

The model procedure deals with an emergency situation in a nuclear facility highly similar to a power plant. That facility is a nuclear waste disposal plant in Idaho. This plant is designed to convert liquid radioactive waste into solid form through a process called fluidized bed calcination.

Plant operations are governed from a control room of the type familiar to the nuclear power industry. Some idea of the control room configuration is given by Figure 3-1.

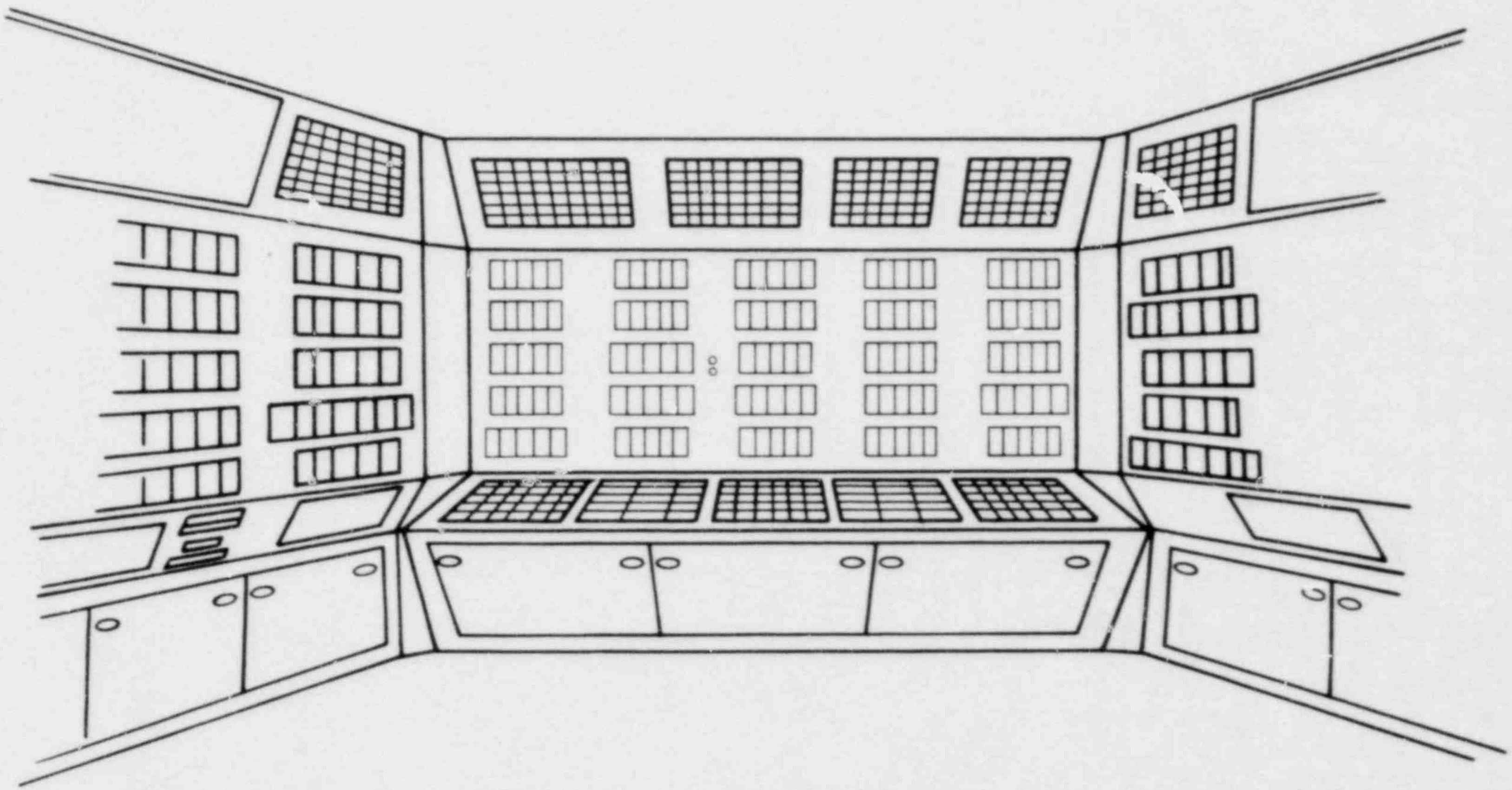


Figure 3-1. Sketch of Control Room in Nuclear Waste Disposal Plant

The model procedure is of the dual-level type planned for two audiences. For the licensed operator, a less-detailed "checklist" procedure is provided on the first page. For the trainee and/or the operator who may need help at various points, detailed procedures are provided on subsequent pages. The detailed procedures are keyed to the checklist by task title and page number.

The detailed procedures give specific direction at the step level, including illustrations that show the location of all relevant controls and indicators.

The procedure itself is geared to a set of flashing red annunciators which denote the existence of this particular kind of emergency. As a result of their training, operators react to the annunciators by obtaining this procedure from the Emergency Procedure Book.

Directions on the first page help the operator interpret the annunciator or group of annunciators to determine the tasks he must perform. Task groups vary among annunciated conditions. Although many of the directions on the first page would be covered by training, they are provided here for reader convenience.

Once the operator identifies the necessary tasks, he follows the checklist. He refers to the detailed procedures only when he needs their information.

3.3.1 Less-Detailed Procedure

EMERGENCY SHUTDOWN CHECKLIST

Entry Conditions:

Rapid Shutdown System (RSS) has been activated, as shown by one or more flashing red annunciators.

Immediate Actions:

1. Identify flashing annunciator(s).
2. Locate annunciator(s) on chart below.
3. Identify all tasks called for by that annunciator or group of annunciators, as indicated by unshaded boxes.
4. To keep your place, mark the first task with an X.

The manual shutdown column on the right is a special case. When performing emergency shutdown tasks, if switches are inoperative or controller settings and readings are not as specified and cannot be adjusted, perform all tasks in the manual shutdown column.

5. Perform all required tasks in top-to-bottom order. If on any task you are unsure of the details, go to the indicated page for help.

EMERGENCY SHUTDOWN TASK ⇩ / ALARM/GROUP ⇨	TSLL/HH-105-1 CALCINER TEMP LOW/HIGH	FSLL-205-1 FLUID AIR FLOW LOW/SHTDOWN	TSHH-305-2 FLUID AIR TO CAL TEMP HIGH/SHTDWN	RSS-6 EMER QUENCH TOWER COOL (TSHH-109-1)	PSLL-105-21 OXYGEN PRESS LOW/SHTDOWN	LSHH-143-1-1 INTERCOOLER 1 LEVEL HIGH/SHTDWN; LSHH-143-2-1 INTERCOOLER 2 LEVEL HIGH/SHTDWN	PSH-334-2 OFF-GAS TO ADSORBERS PRESS HIGH/SHTDWN; PSHH-130-2 OFF-GAS TO FILTERS PRESS HIGH/SHTDOWN; PSHH-243-1 BLO SUCT HDR PRESS HIGH/SHTDOWN; PSHH-105-1 CALCINER V-105 PRESS HIGH/SHTDOWN	TSHH-2214-1 CALCINER CELL TEMP HIGH/SHTDOWN; FSLL-2214-1 CALCINER CELL FLOW HIGH/SHTDOWN	MANUAL SHUTDOWN
1. Begin manual shutdown response (Page 2)	(shaded)	(shaded)	(shaded)	(shaded)	(shaded)	(shaded)	(shaded)	(shaded)	
2. Shut down waste feed flow (Page 3)			(shaded)						
3. Shut down fuel and oxygen flow (Page 4)			(shaded)						
4. Purge feed, fuel, and oxygen lines (Page 5)			(shaded)						
5. Start up quench tower cooling (Page 6)	(shaded)	(shaded)	(shaded)		(shaded)	(shaded)	(shaded)	(shaded)	(shaded)
6. Shut down fluidizing air heaters (Page 7)									
7. Shut down fluidizing air blowers (Page 8)	(shaded)	(shaded)	(shaded)	(shaded)	(shaded)	(shaded)		(shaded)	
8. Shut down off-gas blowers and start up auxiliary blower (Page 9)	(shaded)	(shaded)	(shaded)	(shaded)	(shaded)		(shaded)	(shaded)	

EOP TITLE EMERGENCY SHUTDOWN EOP NO. 1-0
APPROVED BY TITLE PLANT MANAGER DATE 1-20-81
REV NO. 0 DATE OF ISSUE/REVISION 1-20-81 PAGE 1 OF 9

3.3.2 More-Detailed Procedure

EMERGENCY SHUTDOWN PROCEDURES

Begin Manual Shutdown Response

1. Press MANUAL SHUTDOWN button (4).

If plant is not being evacuated, **END OF BEGIN MANUAL SHUTDOWN RESPONSE.**

If plant is being evacuated, continue.

2. Set the following switches to CLOSE. Check that amber lights on switches and semigraphics come on.

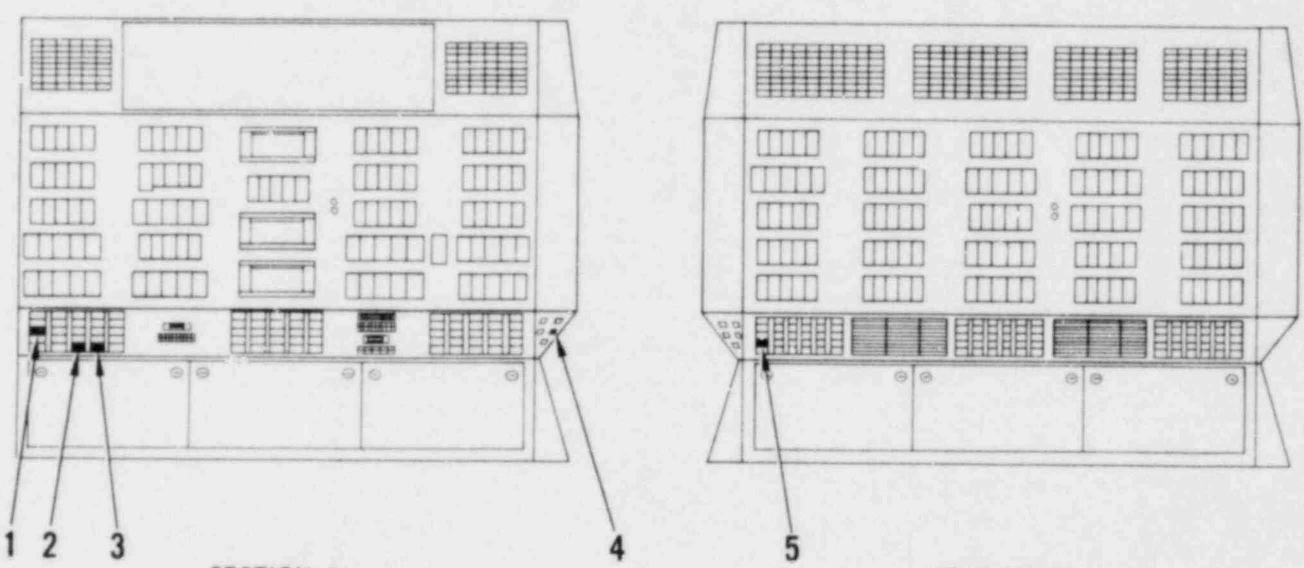
   VES-104 INLET FR VES-102 (2)
   VES-104 INLET FR VES-103 (3)

3. Set HV-103-4 WASTE INLET switch (1) to CLOSE. Check that amber lights on switch and semigraphics come on.

4. Set RECYCLE TO BLEND & HOLD TANKS switch (5) to CLOSE. Check that amber lights on switch and semigraphics come on.

5. Stop any ongoing transfer per PROCESS FEED SOLUTIONS procedure.

END OF BEGIN MANUAL SHUTDOWN RESPONSE



SECTION 1

SECTION 2

CP-NCM-981 CENTRAL CONTROL PANEL

Shut Down Waste Feed Flow

1. ☐ Make sure the following waste feed flow controllers are set to MANUAL mode. Adjust set points to 0.

   FIC-105-1 (1)
   FIC-105-2 (2)
   FIC-105-3 (3)
   FIC-105-4 (4)

If responding to FSLL-205-1, **END OF SHUT DOWN WASTE FEED FLOW.**

If not, continue.

2. ☐ Monitor red pens of the following waste feed flow recorders for readings to start to decrease:

   FR-105-1 (1)
   FR-105-2 (2)
   FR-105-3 (3)
   FR-105-4 (4)

3. ☐ See if reading on TR-105-1 (5) is less than 400° F or rapidly decreasing.

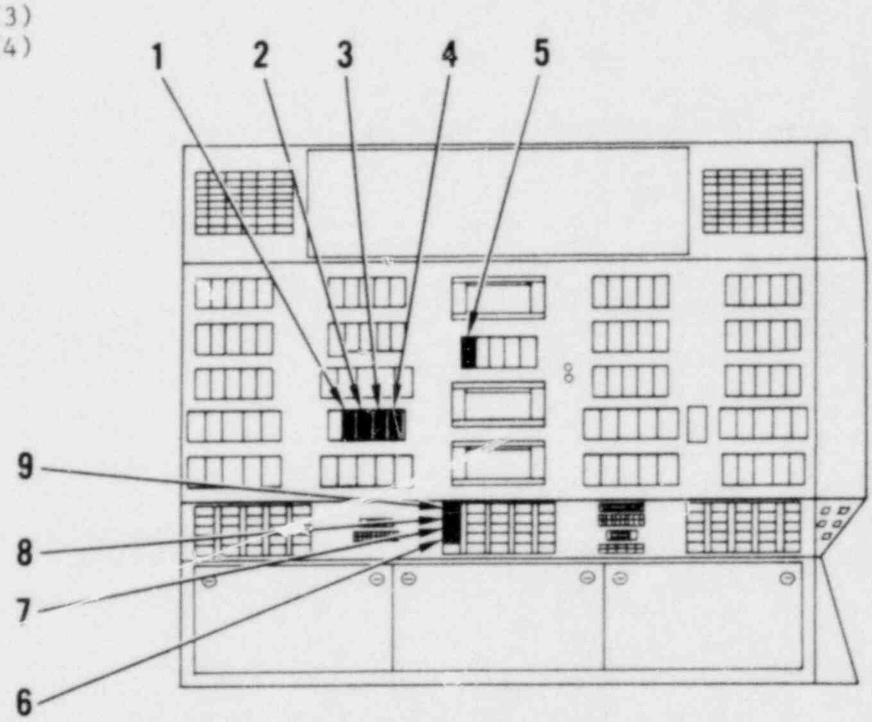
   If reading is less than 400° F or rapidly decreasing, **END OF SHUT DOWN WASTE FEED FLOW.**

   If not, continue.

4. ☐ Set the following FEED LINE WATER PURGE switches to OPEN for 10 seconds, then set to CLOSE:

   FV-105-22 No. 1 (9)
   FV-105-23 No. 2 (8)
   FV-105-24 No. 3 (7)
   FV-105-25 No. 4 (6)

END OF SHUT DOWN WASTE FEED FLOW



SECTION 1 OF CP-NCM-981
CENTRAL CONTROL PANEL

Shut Down Fuel and Oxygen Flow

☐ 1. Set the following fuel and oxygen flow controllers to MANUAL mode. Adjust set points to 0. Monitor until readings decrease to 0.

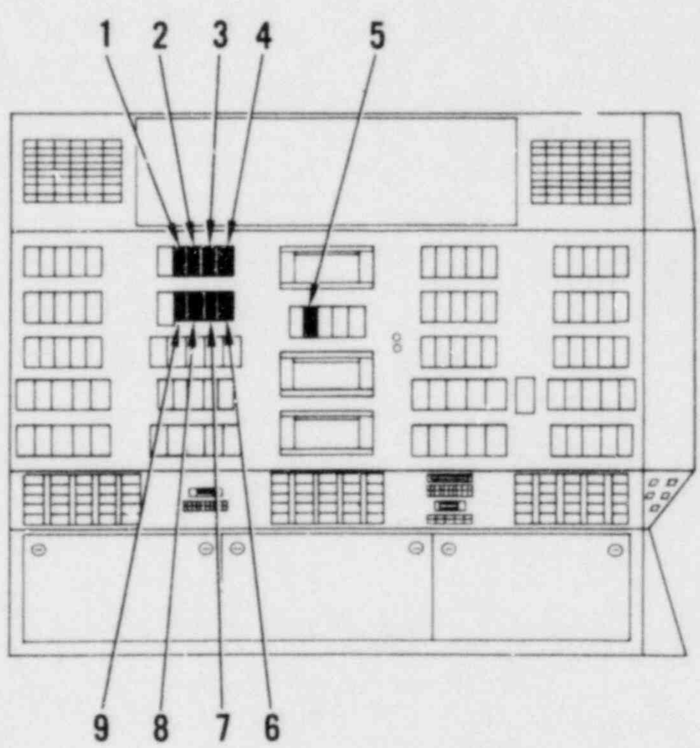
FIC-105-6 (9)	FFIC-105-10 (1)
FIC-105-7 (8)	FFIC-105-11 (2)
FIC-105-8 (7)	FFIC-105-12 (3)
FIC-105-9 (6)	FFIC-105-13 (4)

If responding to FSLL-205-1, **END OF SHUT DOWN FUEL AND OXYGEN FLOW.**

If not, continue.

☐ 2. Set temperature indicator controller TIC-105-1 (5) to MANUAL mode. Adjust set point to 0. Monitor until reading starts to decrease.

END OF SHUT DOWN FUEL AND OXYGEN FLOW



SECTION 1 OF CP-NCM-981
CENTRAL CONTROL PANEL

EOP TITLE EMERGENCY SHUTDOWN		EOP NO 1-0	
APPROVED BY [signature]	TITLE PLANT MANAGER	DATE 1-20-81	
REV NO 0	DATE OF ISSUE/REVISION 1-20-81	PAGE 4	OF 9

Purge Feed, Fuel, and Oxygen Lines

1. ☐ Set the following feed line air purge switches to OPEN. Check that green lights come on.

   AIR PURGE TO FEED NOZZLE NO. 1 (24)
   AIR PURGE TO FEED NOZZLE NO. 2 (23)
   AIR PURGE TO FEED NOZZLE NO. 3 (22)
   AIR PURGE TO FEED NOZZLE NO. 4 (20)

2. ☐ Request that operator in second level operating corridor perform the following:

   a. Monitor the following rotameters for signs of flow:

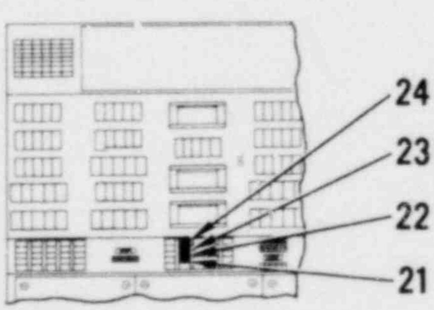
      FI-105-46 (8)
      FI-105-47 (5)
      FI-105-48 (6)
      FI-105-49 (7)

      FI-003-4-19 (4)
      FI-003-4-20 (1)
      FI-003-4-21 (2)
      FI-003-4-22 (3)

      FI-003-4-1 (17)
      FI-003-4-2 (18)
      FI-003-4-3 (19)
      FI-003-4-4 (20)

      If flow is observed, go to Substep c.

      If not, continue.



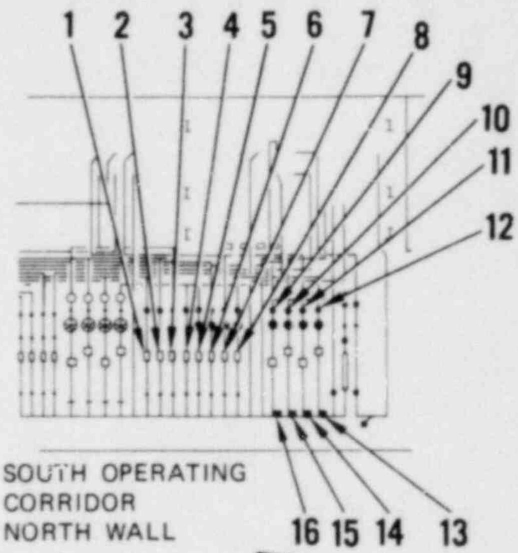
SECTION 1 OF CP-NCM-981
CENTRAL CONTROL PANEL

   b. Open all hand valves on any line that has no flow.

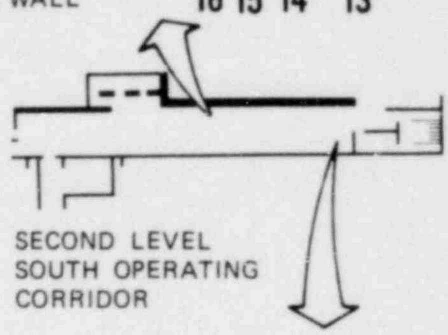
   c. Close the following valves:

      KR-105-1 (12) KR-8 (14)
      KR-105-3 (9) KR-9 (13)
      KR-105-5 (11) KR-10 (16)
      KR-105-7 (10) KR-11 (15)

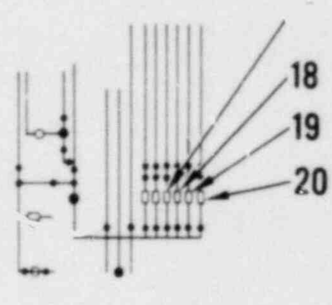
END OF PURGE FEED, FUEL, AND OXYGEN LINES



SOUTH OPERATING CORRIDOR NORTH WALL



SECOND LEVEL SOUTH OPERATING CORRIDOR



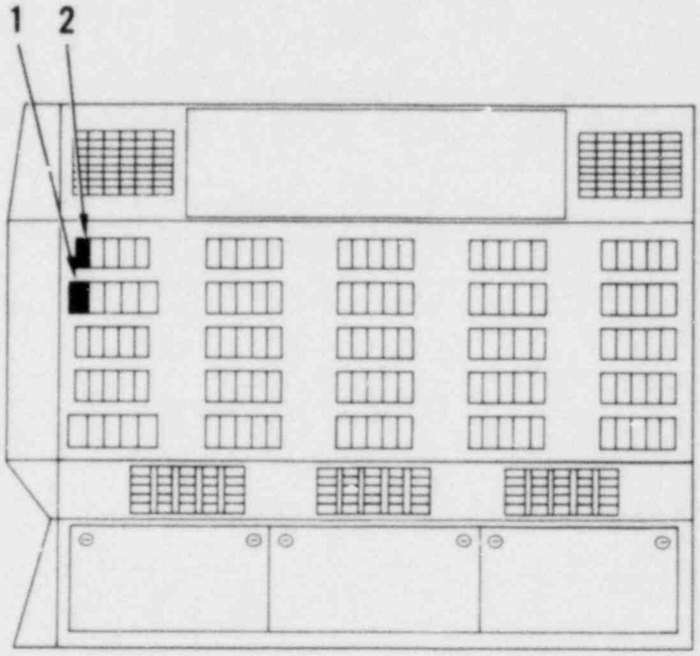
SOUTH OPERATING CORRIDOR SOUTH WALL

EOP TITLE EMERGENCY SHUTDOWN EOP NO. 1-0
APPROVED BY [signature] TITLE PLANT MANAGER DATE 1-20-81
REV NO. 0 DATE OF ISSUE/REVISION 1-20-81 PAGE 5 OF 9

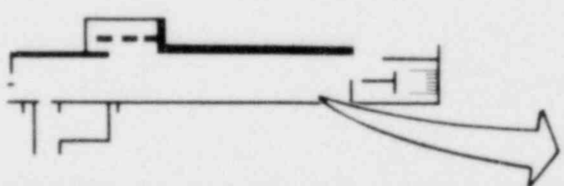
Start Up Quench Tower Cooling

1. Monitor blue pen of TR-109-1 (2) until reading starts to decrease.
2. Monitor red pen of LR-108-1 (1) until reading increases to 80% of chart.
3. Request that operator in second level south operating corridor close treated water valve TW-109-3 (3).

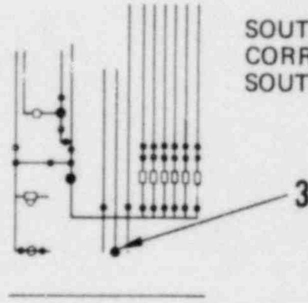
END OF START UP QUENCH TOWER COOLING



SECTION 3 OF CP-NCM-981
CENTRAL CONTROL PANEL



SECOND LEVEL SOUTH OPERATING CORRIDOR



SOUTH OPERATING CORRIDOR SOUTH WALL

EOP TITLE EMERGENCY SHUTDOWN			EOP NO. 1-0
APPROVED BY [signature]		TITLE PLANT MANAGER	DATE 1-20-81
REV NO. 0	DATE OF ISSUE/REVISION 1-20-81	PAGE 6 OF 9	

Shut Down Fluidizing Air Heaters

If responding to TSHH-305-2, go to Step 5.

If not, continue.

1. Set TIC-305-1 (2) to 0.

☐

2. Monitor red pen of TR-305-1 (1) until reading starts to decrease.

☐

3. Set the following fluidizing air heater switches to OFF. Check that amber lights come on.

☐

FLUIDIZING AIR PRE-HTR 305-1 (3)
FLUIDIZING AIR PRE-HTR 305-2 (4)

If responding to TSHH-2214-1 and FSLL-2214-1, go to Step 9, below.

If responding to high intercooler level alarms or high pressure alarms, or if performing manual shutdown, **END OF SHUT DOWN FLUIDIZING AIR HEATERS.**

If responding to any other alarm, continue.

4. Press RESET button(s) (5). Notify shift supervisor that alarm response has been performed.

☐

END OF SHUT DOWN FLUIDIZING AIR HEATERS

5. Set the following fluidizing air heater switches to OFF. Check that amber lights come on.

☐

FLUIDIZING AIR PRE-HTR 305-1 (3)
FLUIDIZING AIR PRE-HTR 305-2 (4)

6. Set TIC-305-1 (2) to 0.

☐

7. Monitor red pen of TR-305-1 (1) until reading starts to decrease.

☐

8. Press RESET button(s) (5). Notify shift supervisor that alarm response has been performed.

☐

END OF SHUT DOWN FLUIDIZING AIR HEATERS

9. Request that second operator look through viewing window (5) to make sure that fire is not present.

☐

If fire is present, notify shift supervisor.

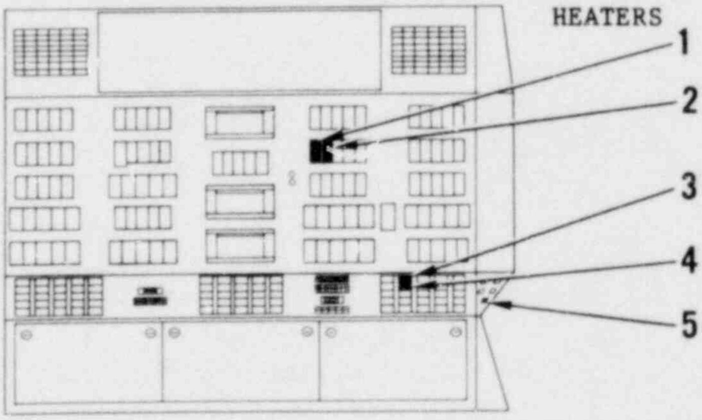
If fire is not present, continue.

10. Press RESET button(s) (5). Notify shift supervisor that alarm response has been performed.

☐

END OF SHUT DOWN FLUIDIZING AIR HEATERS

SECTION 1 OF CP-NCM-981
CENTRAL CONTROL PANEL



EOP TITLE EMERGENCY SHUTDOWN	EOP NO. 1-0
APPROVED BY [signature] TITLE PLANT MANAGER	DATE 1-20-81
REV NO. 0 DATE OF ISSUE/REVISION 1-20-81	PAGE 7 OF 9

Shut Down Fluidizing Air Blowers

1. Set the following switches to OFF. Check that amber lights on switches and semigraphics come on.

   FLUIDIZING AIR BLOWER NO. 1 (2)
   FLUIDIZING AIR BLOWER NO. 2 (3)

If performing manual shutdown response, **END OF SHUT DOWN FLUIDIZING AIR BLOWERS.**

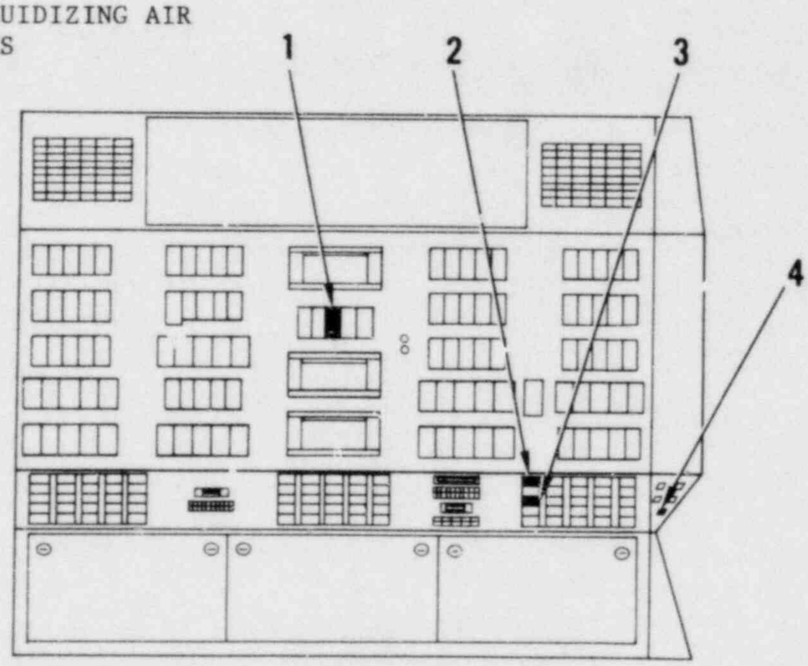
If not, continue.

2. Check that AUXILIARY BLOWER green light on semigraphics comes on.

3. Monitor PR-105-1 (1) until readings start to decrease.

4. Press RESET button(s) (4). Notify shift supervisor that alarm response has been performed.

END OF SHUT DOWN FLUIDIZING AIR BLOWERS



SECTION 1 OF CP-NCM-981
CENTRAL CONTROL PANEL

Shut Down Off-Gas Blowers and Start Up Auxiliary Blower

1. ☐ Set the following off-gas blower switches to OFF. Check that amber lights come on.

   OFF-GAS BLO 243-1 (5)
   OFF-GAS BLO 243-2 (4)

If performing manual shutdown, go to Step 5.

If not, continue.

2. ☐ Check that BLOWER RESET switch (3) is set to NORMAL, and that green light on semigraphics is on. See if AUXILIARY BLOWER green light on semigraphics is on.

3. ☐ Monitor FI-242-1 (6) until flow starts to increase.

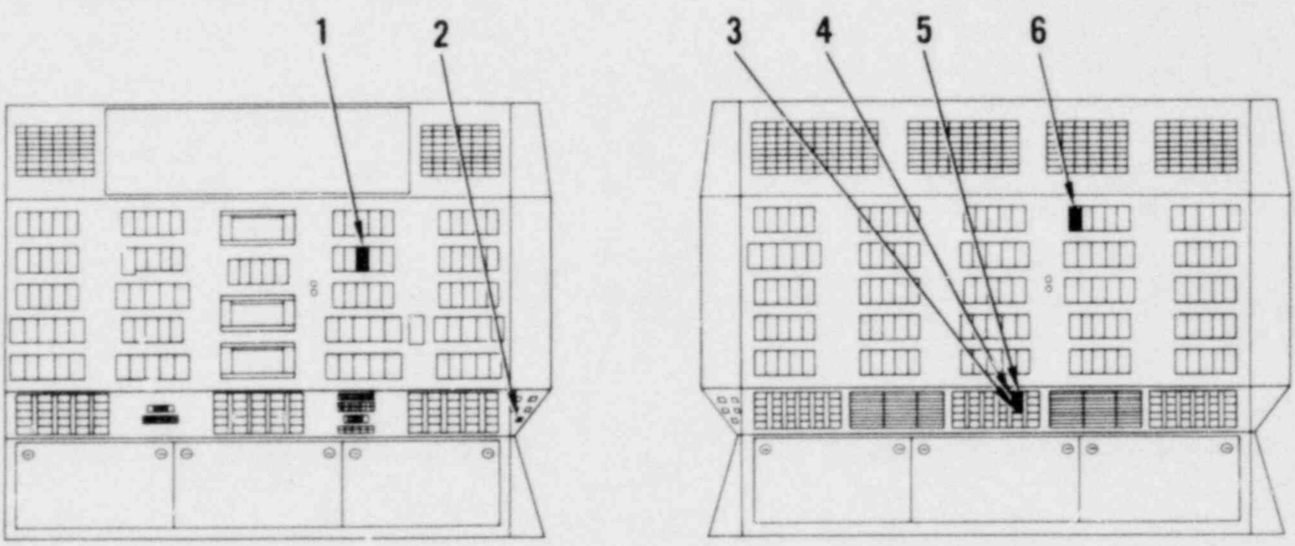
4. Press RESET button(s) (2). Notify shift supervisor that alarm response has been performed.

END OF SHUT DOWN OFF-GAS BLOWERS AND START UP AUXILIARY BLOWER

5. ☐ Check that AUXILIARY BLOWER green light on semigraphics comes on.

6. ☐ Monitor PR-105-1 (1) for reading to increase.

END OF SHUT DOWN OFF-GAS BLOWERS AND START UP AUXILIARY BLOWER



CP-NCM-981 CENTRAL CONTROL PANEL

REFERENCES

1. J.P. Finnegan, T.W. Rettig, and C.A. Rau, Jr., Failure Analysis Associates, "The Role of Personnel Errors in Power Plant Equipment Reliability," EPRI AF-1041. Available through Research Reports Center (RRC), Box 10090, Palo Alto, CA 94303.

2. J.P. Finnegan, Failure Analysis Associates, "Workshop Proceedings: The Role of Personnel Error in Fossil Fuel Power Plant Equipment Reliability," EPRI AP-1470. Available through Research Reports Center (RRC), Box 10090, Palo Alto, CA 94303.

3. A.D. Swain and H.E. Guttman, Sandia Laboratories, "Handbook of Human Reliability Analysis With Emphasis on Nuclear Power Plant Applications," USNRC Draft Report NUREG/CR-1278, October 1980. Available in NRC PDR for inspection and copying for a fee.

4. Robert Sugarman, "Nuclear Power and the Public Risk," Spectrum, November 1979. Available in public technical libraries.

5. Kay Inaba and others, Serendipity, Inc., "Project PIMO Final Report," TR-69-155 (AD-852-101), Volumes I-VIII, May 1969. Available through Space and Missile Systems Organization, Air Force Systems Command, Norton Air Force Base, California.

6. Joseph L. Seminara, Wayne R. Gonzalez, and Stuart O. Parsons, Lockheed Missiles & Space Company, "Human Factors Review of Nuclear Power Plant Control Room Design," EPRI NP-309, November 1976. Available through The Electric Power Research Institute, 3412 Hillview Ave., Palo Alto, CA 94304.

7. U.S. Department of Defense, "Technical Manual Writing Handbook," MIL-HDBK-63038-1 (TM), 1 May 1977. Available through Defense Documentation Center (DDC), Cameron Station, Alexandria, Va. 22314.

NRC FORM 335 (7-77)

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

1. REPORT NUMBER *(Assigned by DDC)*
NUREG/CR-1999

4. TITLE AND SUBTITLE *(Add Volume No., if appropriate)*
Human Engineering Guidelines for Use in Preparing Emergency Operating Procedures for Nuclear Power Plants

2. *(Leave blank)*

3. RECIPIENT'S ACCESSION NO.

7. AUTHOR(S)
Frank Fuchs, Julia Engelschall, Greg Imlay

5. DATE REPORT COMPLETED

MONTH	YEAR
March	1981

9. PERFORMING ORGANIZATION NAME AND MAILING ADDRESS *(Include Zip Code)*
XYZYX Information Corporation
21116 Vanowen Street
Canoga Park, CA 91303

DATE REPORT ISSUED

MONTH	YEAR
April	1981

6. *(Leave blank)*

8. *(Leave blank)*

12. SPONSORING ORGANIZATION NAME AND MAILING ADDRESS *(Include Zip Code)*
U. S. Nuclear Regulatory Commission
Division of Human Factors Safety
Office of Nuclear Reactor Regulation
Washington, D. C. 20555

10. PROJECT/TASK/WORK UNIT NO.

11. CONTRACT NO.
Fin No. B6872

13. TYPE OF REPORT
Technical

PERIOD COVERED *(Inclusive dates)*

15. SUPPLEMENTARY NOTES

14. *(Leave blank)*

16. ABSTRACT *(200 words or less)*

Emergency procedures for nuclear power plants were examined to include considerations of the development process, the circumstances of use, and the state of the art relative to procedure design. Recommendations were then formulated for NRC use in behalf of the entire industry.

This report is presented in three sections. In Section 1, operator errors are analyzed for the purpose of showing how they can be affected by written procedures. In Section 2, an assessment is made of the emergency procedures from nine nuclear power plants. Deficiencies are examined in terms of the kinds of errors they could invite. In Section 3, recommendations are made on behalf of improved procedures throughout the industry. The recommendations include a model emergency procedure.

17. KEY WORDS AND DOCUMENT ANALYSIS

17a. DESCRIPTORS

17b. IDENTIFIERS/OPEN-ENDED TERMS

18. AVAILABILITY STATEMENT
Unlimited

19. SECURITY CLASS *(This report)*
Unclassified

21. NO. OF PAGES

20. SECURITY CLASS *(This page)*
Unclassified

22. PRICE
$