

**Brown & Root, Inc.** Post Office Box Three, Houston, Texas 77001



Reply Address

J. V. Stephens  
Bldg. 23, Room 240  
Electrical Engineering Dept.  
Power Division  
Brown & Root, Inc.  
P.O. Box 3  
Houston, Texas 77001

July 31, 1979

Mr. Roger Mattson, Director  
Division of System Safety  
Nuclear Regulatory Commission  
Washington, D.C. 20555

Three-Mile Island Incident  
Operator Interface

Dear Mr. Mattson:

The events at Three Mile Island in which some of the problems, according to some sources, have been attributed to operator error and instrumentation deficiencies led me recently to look back on some of my thoughts during the early stages of development of IEEE-566 "Guide for the Design of Display and Control Facilities for Central Control Rooms for Nuclear Generating Stations".

I believe that some of these thoughts which center around the operator-control interface could be of interest and am therefore enclosing a copy of my letter dated May 20, 1976 and copy of an early draft of P566/D3B March 1976. My letter of May 20, 1976 was an in-depth and lengthy review of the P566/D3B draft in which I discussed some of the problems that could confront the operator during and after an accident.

On page 5 of my letter of May 20, 1976 I made a number of recommendations. Among them the need for safety systems to be so designed to ensure that under post accident conditions and failure of automatic systems, the operator will never be overburdened with necessity of suddenly having to rapidly execute a large number of emergency manual operations all needed at the same time - since this can only aggravate an already tense situation and increase the possibility of an operating error. Included also was the suggestion for a vigorous analysis of expected operator actions during the post accident period under trauma and greater use of simulators to evaluate operator performance.

509 242

X6501  
ADD:  
P. COLLINS  
w/ENCL

7908070 553

Mr. Roger Mattson  
Page 2

For reasons having to do with the difficulty of consensus but more probably with the political climate of that time none of these recommendations ever found their way into the final text of IEEE-Std.566 "Guide for the Design of Display and Control Facilities for Central Control Rooms for Nuclear Generating Stations" when it was published in July 1977.

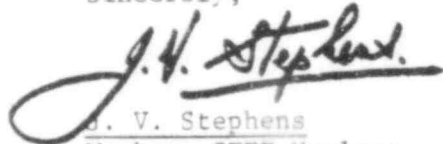
While the final analysis of the Three Mile Island accident might reveal certain factors only generically related to the concerns expressed in my letter of May 20, 1976, I believe these concerns are pertinent within the overall objective of minimizing operator error.

With this in mind I respectfully pass on to you the enclosed material containing some of my thoughts and concerns which may be more acceptable in the political climate of today and may be useful to those on your staff working on recommendations resulting from the Three Mile Island accident.

Please note the thoughts expressed in this letter are entirely my own, are meant to be helpful, and based on considerable experience in this area.

Your time and consideration is appreciated.

Sincerely,



J. V. Stephens  
Member, IEEE Nuclear  
Power Subcommittee  
Phone (713) 678-5148

JVS/kam

cc: H. R. Denton, NRC  
J. MacMillan, Babcock & Wilcox  
W. G. Kuhns, G.P.U.  
H. H. Woodson, IEEE  
I. G. Easton, IEEE  
J. B. Sullivan, IEEE/PES/PGC  
J. T. Boettger, IEEE/PES/NPEC  
A. J. Spurgin, IEEE/PES/NPPC&P  
E. F. Chelotti, IEEE-ANSI

509 243

*J. V. Stephens*

**Brown & Root, Inc.** Post Office Box Three, Houston, Texas 77001



May 20, 1976

Mr. A. J. Spurgin  
Chairman, NPPC & P, WG & SC1.2  
General Atomic Company  
P. O. Box 81608  
San Diego, California 92138

**Comments**

Guide for the Design of Display and  
Control Facilities for Central Control  
Rooms of Nuclear Generating Stations  
IEEE-P566/Draft 3B March 1976

Dear Tony:

I have reviewed the above draft and am returning a copy herewith marked up with my comments. Following is an amplification of these comments coupled with a discussion where appropriate.

GENERAL

1) Minor errors in spelling; word omissions, and wrong word usage occurs throughout the text. Suggested corrections are marked up on the enclosed copy.

2) Subsection 7.6.1 Safety System Status.

Needs to be reworked in its entirety.

3) Subsection 7.6.2 Redundant Display Information.

The statement "redundant (i.e. two pressure alarms)" needs to be carefully qualified.

4) Section 7.11 Internal Security.

This could be more explicitly stated by a slight change in wording.

✓ 5) APPENDIX - Example of Operator Sensory Overload in Operation of Safety Systems.

Not the best example. Needs careful rework.

509 244

Mr. A. J. Spurgin

page 2

I consider the APPENDIX to be the most disturbing and shall therefore start with this.

1) APPENDIX - Example of Operator Sensory Overload in Operation of Safety Systems. ✓

The intent of this Appendix, presumably, is to show a classical example of a situation where during or after the occurrence of an accident, the operator or operators may suddenly be called upon to perform a large number of operations all at once. In this situation, considering the electrified atmosphere created by the accident, the psychological response of the operator at that time, the possible need under certain circumstances to act quickly with a sense of immediacy - could, conceivably lead to an operating error of serious proportions. It is the fundamental objective of our document to provide guidelines for the organization, integration and coordination of all controls and displays for use by the operator so as to facilitate his ability to operate the plant efficiently and more importantly, to reduce to the greatest extent practical any potential for operator error by considering possibly, among other situations, the very example postulated in the Appendix.

The example, unfortunately, falls down in several ways. The statement "simultaneous operator manual action" in the second paragraph of the example obviously implies that all the events Nos. 1 through 10 could occur so close together in time as to overload the operators with too many tasks to perform practically all at the same time. Even though it is true that events could proceed in an unforeseen way (in which case, if it is unforeseen, I don't know what we can do about it, because a certain amount of "forseeing" is basic to the design process) it is extremely hard to imagine, even with the most sympathetic stretch of the imagination that all these events could possibly occur around the same time. If they did, it could only be the result of a series of incredible fortuitous events that not even the NRC, I believe, have ever postulated in their design reviews, or alternatively, the end result of extremely irresponsible design.

While on the subject of design you know as well as I do that it is not possible to produce the perfect design of information and control systems to perfectly satisfy every event postulated. The perfect design of say an arrangement of control and display systems to perfectly satisfy event A may conflict with the perfect design requirements to perfectly satisfy event B, C, or D, etc. depending on the number and different type of events postulated and considered in the design. Of course, there are certain DBE's that must be designed against and means must also designed to limit their consequences should they occur. Aside from the mechanical systems, in our case we have an orderly arrangement of display and control devices which would enable the operator to perform functions with minimum potential for error even when he is in a state of shock or still recovering from it.

509 245

Mr. A. J. Spurgin  
page 3

However, there are a number of events which, while possible, are so improbable that to attempt to organize our control and display facilities around it with the objective of minimizing as much as possible any potential for operator error could only be done at the sacrifice of other arrangements suited for more possible events. Therefore, design consists of compromises and trade-offs as for example where an arrangement of control and display devices for say, three specified Design Basis Events could give a confidence factor of say 90%, 95%, and 99% of freedom from operator error, other events much lower in the scale of probabilities and consequences will necessarily have to tolerate confidence factors of a lower order.

In the example given, emphasis should be more on good plant design to assure that all the events listed to not occur around the same time than on how we can organize our control and display systems to help him cope with a situation which is so incredible as to be close to the realm of impossibility. My reasons for this viewpoint is based on the considerable differences in expected elapsed time between the events postulated. For example:

- a) Event 4 - Switchover from ECCS water tank to reactor containment building sump.

A time period of something in the order of 20-40 minutes would elapse after the onset of the accident before the tank would be depleted to the point of requiring manual or automatic transfer to the containment sump. This time period will vary somewhat, depending on the severity of the break, whether sprays are in operation, and whether all or only a portion of the redundant safety injection trains are running. I have checked with some of the PWR plants that I have worked on in the past and also with some of our nuclear people. The opinion is that 20-40 minutes is an order of magnitude fairly representative of PWR plants in this country. What I am saying here is that this event is one that involves a time period, after the accident, of minutes or at the most hours, whereas events No.'s 7 or 8 if they occur will take place generally at least several days after the accident. Thus, the incongruity of the assumption that events No.'s 4, 7 and 8 could occur so close together in time as to strain the manual capabilities of the operators.

While on this subject, I would mention that I think there is a trend towards automatic rather than manual realignment of suction valves to the containment sump, although some plants may have only the manual feature. The event described in the example should therefore be qualified to the extent that it indicates manual transfer where the system is either manual, or, if automatic, where the automatic system failed.

Mr. A. J. Spurgin  
page 4

b) Event 7 - Replenishment of diesel fuel and makeup of cooling water.

From IEEE-308-1974 page 8, Section 5.2.4 (6) Energy Storage, it can be seen that sufficient stored energy (fuel) must be available at the site to operate standby power sources (diesels) at accident loads for a period of which the minimum is not less than (7) seven days. That is to say that as a minimum, (7) seven days of fuel supply must be available at the site. Admittedly, a situation could arise in which, because of a violation of company procedures or technical specifications, only a few hours or few days supply of fuel was available at the time of the accident at which time of course all offsite power supplies was lost. But I do not think this was the intent behind the example. What I have tried to point out here is the sheer improbability of a coincidental situation requiring operator action to replenish diesel fuel which is normally done days after the accident, with the switchover of the ECCS water tank to the containment sump which occurs either manually or automatically after 20 or 40 minutes or at the most a matter of hours after the accident. In regard to the cooling-water I am not sure what this means. Presumably it means engine jacket cooling water.

c) Event 8 - Start H<sub>2</sub> Recombiner System.

Again the time at which a switchover from the ECCS tank to the sump is needed, and the time at which the generation of hydrogen in the containment will have reached a level requiring activation of the recombiner are so far apart that it would be incredible to think that the two events could occur even approximately around the same time, leave alone simultaneously. On some of the PWR plants that I have checked, the elapsed time after the occurrence of an accident when activation of the recombiner is needed is calculated to be something between 5-15 days. This again, contrasts with the time to switchover from the ECCS Tank to the sump which at most is measured in hours rather than days.

---

Tony, I have tried here, as best I can, to bring to your attention the implausibility of all the events indicated in the example occurring at the same time. It is true that a possibility exists where the time to manually replenish diesel fuel and the time to activate the recombiner could occur approximately around the same time since for each event we are talking in terms of days.

Mr. A. J. Spurgin

page 5

However, even here we must grant the operators a certain amount of intelligence. Where several days have elapsed after the accident and, assuming the accident is under control, then it is reasonable to assume that the operators have sufficiently recovered from the shock to have their wits about them to monitor the trend of hydrogen generation and the rate of fuel depletion by means of instruments available in the control room some of which form part of the Post Accident Monitoring System. Thus, the operators will plan their operations. They may start replenishing fuel in the diesel tank a day or so before it is depleted - they anticipate and try to take prior action rather than wait for everything to come to a head at the same time.

There are other questionable events in the example shown in the Appendix but it would take me too long to discuss them here. However, the Appendix does have some very positive aspects in that it brings to mind somewhat, forcibly, the crucial need to consider certain requirements which have been conspicuously omitted from our document.

As I see it these are:

- (i) The need to include somewhere within our document criteria to the effect that the design of safety systems shall ensure to the maximum extent practical that post accident events designed to require manual actions by the control room operators shall be so spaced in time to obviate the necessity of a large number of manual operations at any one given time.
- (ii) The need to include within the document recommendations to the effect that an analysis should be made of expected operator actions during the post accident period using time as a base. There could be several analyses based on the postulated DBE's.
- (iii) The need to include some words within our document on the advisability of considering the use of a simulator and/or mockup arrangement early in the design to evaluate the performance of both the operator and the control and display interface for both accident and post accident conditions.

If after reviewing these rather critical comments you decide that you still wish to retain the Appendix, I will strongly suggest that the events described be more plausibly related time-wise. They should have a reasonable possibility of occurring within the first (24) twenty-four hours after the accident. It will be during this period that, I should think, that the operators will still be under severe emotional strain with possibly more potential for operator error rather than several days after the event, by which time they might have got used to the idea or alternatively gotten to hell out of it.

Mr. A. J. Spurgin  
page 6

If this Appendix is unchanged it will be a serious flaw to what I think is generally a good document. A pity, indeed, considering the persevering efforts and infinite patience expended by yourself and others during the nearly three years of development and preparation of this document.

Since it would be unfair to expect any one member to put together such an Appendix unaided, I would suggest that you call together a small number of members of the group knowledgeable in the operations required during accident and post accident conditions so that a revised Appendix could be prepared as a joint effort. The revised Appendix should have a clear purpose and relevancy to the document in that it should advocate, recommend or require the system designer to consider, analyse, reduce the potential, or try to do something about such a hypothetical situation (i.e. foresee it) early in the design stage.

The only alternative is to leave the Appendix out altogether.

2) Page 14 - Section 7.11 Internal Security.

The existing wording does not sound right. Three alternatives are shown on the marked up copy.

3) Page 13 - Subsection 7.6.2 Redundant Display Information.

Third Sentence:

"These alternate sources of confirming information can be in the form of redundant (i.e., two pressure alarms) or diversified (i.e., one breaker tripped alarm and one low pressure alarm or indication) information."

Comment:

- a) The "one breaker tripped alarm and one low pressure alarm . . .", is excellent as corroborating information. This is because we are dealing with cause and effect which are logically as well as sequentially related. The breaker feeds power to the motor which drives the pump which raises the pressure in the fluid. A low pressure indication with the breaker still closed could possibly be a ruptured pipe or maybe a faulty pressure switch. But a low pressure alarm accompanied by an open breaker not only confirms the fact of low pressure but also tells the operator "why" the pressure is low. Why the breaker tripped could be another matter. The point is that the information the operator has received is pretty reliable i.e. that there is definitely low pressure in the system.
- b) Unlike the "breaker tripped alarm and low pressure alarm", the statement in the first part of the section under review i.e. "can be in the form of redundant (i.e. two pressure alarms)"



Mr. A. J. Spurgin

page 7

can cause problems unless clarified. There is a point of fact no confirming information at all if one of the pressure alarms indicate say, low pressure and the other is passive. Which of these two is he to believe? It is plausible that the one that indicates low pressure is the true situation and the one that was passive the result of a defective pressure switch. Alternatively the one that indicates low pressure could be the result of a spurious signal. The operator in this case would have to verify the situation by looking at other indicators if related to the system under observation. In the end he might have to send somebody out to investigate. Clearly this does not lend itself to rapid verification. As a minimum, I should think you need either three indicators or pressure alarms with operation of two or more to verify the situation or, one pressure alarm which can be activated only by two or more pressure switches to avoid false indication by spurious operation of one switch. This is, of course, the well known 2 out of 3 concept.

4) Page 12 & 13 - Subsection 7.6.1 Safety System Status

I appreciate that it is not easy to do full justice to R.G. 1.47 and IEEE-279 in a couple of sentences, however, the wording in Subsection 7.6.1 which is based on the foregoing does leave something to be desired. The first and third sentences of this section seem to be saying the same thing. The second is superfluous. The fourth and fifth sentences appear to contain the basic message. In the sixth sentence, the inclusion of, ". . . more than once a year" in a document of such broad scope as ours, seems questionable. I cannot promise but if I can get the time, I will try to work up a substitute.

5) One last item which is more of an interesting observation than anything else. Compare the following :

a) Page 5 - Subsection 4.3 Displays (our document)

Devices which convey information to the operator.

b) IEEE 308-1974 - Page 5 Section 3 Definitions

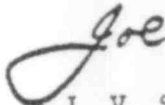
Indicators. Devices that display information to the operator.

The unfortunate point about our definition is that it does not say that the information conveyed to the operator is by video means which is the quintessence of a display. An evacuation horn in a plant, which by itself is purely an audio form of information, does convey information to the operator and is also a device - but it certainly is not a display as the words of the definition in our document would have you believe.

Mr. A. J. Spurgin  
page 8

I hope these comments will be of assistance. Best regards.

Sincerely,

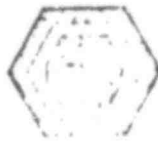


J. V. Stephens  
Staff Manager - Electrical  
Power Engineering

JVS/ml

cc: J. R. Hall  
W. G. Schwartz  
R. A. Schmitter  
D. Tondi

509 251



*J.V. Stephens*  
Rec'd 4/28/76

GENERAL ATOMIC COMPANY  
P.O. BOX 31038  
SAN DIEGO, CALIFORNIA 92138  
(714) 453-1000

April 26, 1976

*J.V. Stephens.*

Members of the P.566 Working Group

Please find attached a copy of the latest draft of the P.566 document. Please would you review the copy for errors and areas of the document that have been added since our last meeting in Florida. We have already taken a vote on the remaining portions of the document and the vote was unanimous. The sections that have been altered are:

- 7.6.1 Safety System Status
  - 7.6.2 Redundant Display Information
  - 7.10 Communications
  - 7.11 Internal Security
- Appendix

In discussions with C. Chiappetta, we have decided to see whether we can get the document approved at the next N.P.E.C. meeting. In order to achieve this objective, all the ballots should be returned from the non-voting members, the comments should be resolved in terms of what is now contained in the Draft D5B.

I will be asking some of you to try to get the ballots returned and others to resolve comments. I will be sending out a letter on this shortly. Please let me have your comments as soon as possible on the document. The document should be in the NPEC members hands 20 days before the next meeting, which is 3-4-5 of August in San Diego.

Yours sincerely,

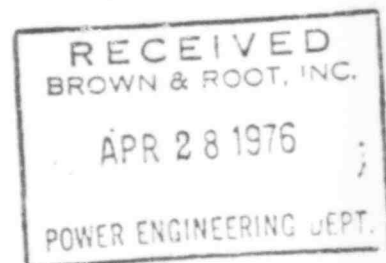
*Tony*

A. J. Spurgin

AJS:mat  
Attachment

CC: C. Chiappetta  
M. I. Olken

509 252



*J.V. Stephens*  
*rec'd 4/28/76*

P566 / D3B

Guide for the Design of Display and Control  
Facilities for Central Control Rooms of  
Nuclear Generating Stations

Draft 1	October 1974
Draft 1A	February 1975
Draft 1B	April 1975
Draft 1C	May 1975
Draft 2	July 1975
Draft 3A	January 1976
Draft 3B	March 1976

*Comments as  
marked and as  
indicated in attached  
letter May 1976 to  
A.J. Spurgeon.  
J.V. Stephens  
5/19/76*

Work performed under the auspices of the Power Generation  
Committee (PGC) and the Nuclear Power Engineering Commit-  
(NPEC) by a combined Working Group of the Nuclear Power Pla-  
- Control, Protection and Automation Subcommittee and of NPEC  
SC1.2.

## TABLE OF CONTENTS

FOREWORD . . . . .	1
1.0 SCOPE . . . . .	3
2.0 PURPOSE . . . . .	3
3.0 REFERENCES . . . . .	3
3.1 Specific to Document . . . . .	3
3.2 Other References . . . . .	3
4.0 DEFINITIONS . . . . .	5
4.1 Availability . . . . .	5
4.2 Central Control Room . . . . .	5
4.3 Displays . . . . .	5
4.4 Emergency Operations Area(s) . . . . .	5
4.5 Functional Area . . . . .	5
4.6 Information . . . . .	6
4.7 Normal Operations Area . . . . .	6
4.8 Operating Mode . . . . .	6
4.9 Operator . . . . .	6
4.10 Safety System . . . . .	6
4.11 Supporting Operations Area(s) . . . . .	6
5.0 DESIGN BASES . . . . .	7
5.1 General . . . . .	7
5.2 Content . . . . .	7
6.0 USAGE ANALYSIS . . . . .	9
7.0 FUNCTIONAL REQUIREMENTS . . . . .	10
7.1 General . . . . .	10
7.2 Display Facilities . . . . .	10
7.3 Control Facilities . . . . .	12
7.4 Device and Display Identification . . . . .	12

CONTENTS (Continued)

7.5	Convention for Control Devices . . . . .	12
7.6	Display and Control Facilities - Special . . . . .	12
7.7	Area Arrangement . . . . .	14
7.8	Device Arrangement . . . . .	14
7.9	Equipment or System Status . . . . .	14
7.10	Communications . . . . .	14
7.11	Internal Security . . . . .	14
Table 1	. . . . .	16
APPENDIX	. . . . .	17

## Facilities

# Guide for the Design of Display and Control Facility for Central Control Rooms of Nuclear Power Generating Stations

## Foreword.

The nuclear power plant control room is the central location of the operator-power generation interface. It is the location where the plant operating personnel must make decisions and take actions necessary to ensure the safe, efficient operation of the plant.

The assignment of functions to an operator, the type, layout and accessibility of the necessary information and action devices, the design for the comfort and protection of the operator, and the degree to which automatic control is utilized must all be established, recognizing the response capabilities of the operator, so as to optimize the use of his judgement as a valuable resource. *in ?*

The selection of specific display and control equipment as well as the determination of information formats and control switchboard layouts has traditionally been and undoubtedly will continue to be largely the prerogative of the individual user. Also, the technical operating requirements for individual plant systems are determined and established largely by the individual system designers. Therefore, the successful integration of the requirements into a coordinated design that will meet operating and regulatory objectives requires that common guidelines be generated to guide all involved designers in making necessary selections and decisions. It is to this end that this document sets forth such guidelines.

The committee recognizes that the method of dealing with functional classification of displays and controls is important. Table 1 of the document is one of several methods which the designer may use to classify

and group the various control room displays and controls. Investigations were made by the committee in an effort to quantify the relative values of various types of controls and displays. The committee recommends that a systematic approach to determine the classification of the control and display facilities be used.

The members of the working group at the time of development of <sup>THIS</sup> document were:

Chairman, A. J. Spurgin

O. M. Anderson  
C. L. Cobler  
W. A. Coley  
R. S. Darke  
J. R. Hall  
D. A. Hansen  
W. Kerchner  
G. Lilly  
J. A. List  
J. Owen  
R. W. Park

R. A. Palmer  
D. S. Peikin  
R. J. Reiman  
H. F. Reischel  
R. M. Reymers  
D. C. Richardson  
R. A. Schmitter  
J. V. Stephens  
M. D. Sulouff  
V. D. Thomas  
W. E. Wilson  
P. Woodard



## 1.0 SCOPE

This document establishes guidelines to be used by power plant system designers in selecting information and control devices to be made available in the central control room, and in determining how and where they shall be made available so that they can most reliably and quickly be used by the operator. The guide addresses the functional requirements of the information systems, controls and displays, but not the selection of specific devices or equipment. It does not apply to the physical design of the control room enclosure or structures mounted therein.

## 2.0 PURPOSE

To provide uniform guidelines for the functional selection, coordination and organization of control and information systems in a nuclear power plant central control room.

## 3.0 REFERENCES

The reference section is divided into two parts, the first contains the references mentioned in this document, and the second contains a set of related references to which reference is not made.

### 3.1 Specific to Document

- IEEE 279-1971 Protection Systems for Nuclear Power Generating Stations *CRITICIA FOR*
- IEEE 308-1974 Class IE ~~Electrical~~ <sup>Power</sup> Systems for Nuclear Power Generating Stations *CRITICIA FOR*

### 3.2 Other References

NRC General Design Criteria (10CFR50, Appendix A)

509 258

Criterion 13 Instrumentation and Controls

Criterion 19 Control Room

IEEE Standards and Guides

~~366-1971~~

336

Installation, Inspection and Testing Requirements for Instrumentation and Electric Equipment during the Construction of Nuclear Power Generating Stations.

✓ 338-1975

Criteria for the Period Testing of Nuclear Power Generating Station Class IE Power and Protection Systems

hyper. Trial-Use

✓ 384-1974

Trial-Use Standard Criteria for Separation of Class IE Equipment and Circuits

420-1973

Trial-Use Guide for Class IE Control Switchboards for Nuclear Power Generating Stations

ANS Standards

ANSI N660

Criteria for Safety Related Operator Actions  
(Document is still in the review process)

4.0 DEFINITIONS

4.1 Availability

Relates to the accessibility of information to the operator on an instantaneous, "sequenced" or as "called for" basis. It is not the intention of this document to address hardware (system) availability.

*instantaneous*

4.2 Central Control Room

A continuously manned, protected enclosure from which actions are normally taken to operate the nuclear generating station under normal and abnormal conditions.

4.3 Displays

Devices which convey information to the operator.

*visual - see attached letter*

4.4 Emergency Operations Area(s)

A functional area(s) allocated for the displays used to assess the status of safety systems and the controls for manual operations required during emergency situations.

4.5 Functional Area

A location or locations designated within the control room to which components relating to a specific function or functions are assigned.

*suggest "display & control devices" in lieu of components. This will make it consistent with 4.7 i.e. displays & control on page 6.*

POOR ORIGINAL

509 260

4.6 Information

Data describing the status and performance of the plant.

4.7 Normal Operations Area

*normal?*

A functional area allocated for those displays and controls necessary for the tasks *often performed* ~~frequently involved~~ during plant startup, shutdown and power operation modes.

4.8 Operating Mode

The nuclear power plant modes as defined by the technical specifications for the plant.

4.9 Operator

A person licensed to operate the plant.

4.10 Safety System

The collection of systems which perform to mitigate the consequences of design basis events.

4.11 Supporting Operations Area(s)

Functional area(s) allocated for supporting plant control and display functions that are required infrequently.

## 5.0 DESIGN BASES

### 5.1 General

The design bases for the control and display facilities in the central control room should be established and documented, before beginning the detailed control room design. This establishes the bases for making design decisions as well as making judgements on the appropriateness and adequacy of information and its presentation. *together with controls and their orientation.*

### 5.2 Content

The following are examples of items to be considered as part of the design bases. The design bases need not be limited to these items:

- 5.2.1 The operating modes for which the central control room display and control facilities should be designed.
- 5.2.2 The number of operators and the responsibilities assigned to them under each operating mode.
- 5.2.3 The functional areas, into which the control room is to be organized, these may include the normal, emergency and supporting operations areas.

Note, these functional areas need not be physically separate.

- 5.2.4 The basis for grouping of display and control devices within any functional area.

509 · 262

- 5.2.5 The limiting number of display devices, by type, established as a design goal for each functional area of the control room. ~~(This is to avoid~~ <sup>prevent</sup> operator sensory saturation. (An example of sensory overload is contained in the Appendix.)
- 5.2.6 A listing of the safety related display and control instrumentation (including Post Accident Monitoring instrumentation) for which specific requirements are already established by regulatory requirements, industry standards and/or safety analysis reports.
- 5.2.7 The requirements which are mandated by, or directed by, user company policies and/or contracts.
- 5.2.8 The anthrometric <sup>anthropometric</sup> relationships to be used for design of the control boards.
- 5.2.9 The list of functions, which are shared between the central control room and the remote shutdown facility, the status of which are to be displayed at both locations.
- 5.2.10 The sequence of events for the postulated design bases events.
- 5.2.11 Data to be used for trend and historical record purposes.

## 6.0 USAGE ANALYSIS

The designer should establish and document a systematic method for determining the availability, priority, importance, <sup>and</sup> location of the control devices and displays.

The following items should be considered:

- a) Plant systems
- b) Operating modes
- c) Frequency of use
- d) Response time
- e) Safety classification
- f) The grouping of displays and control devices in an operational area.
- g) Special requirements

One systematic approach is depicted by use of Table 1. The designer, in this approach, first lists all the plant systems and completes the tabulation for each system. Each control device and display within a specific system, is then listed in a separate tabulation and the appropriate determination of usage made. When such a system is properly applied and the results analyzed, patterns will emerge to assist the designer in the physical allocation of switchboard space and assignments of operator controls and displays. Compliance with the design basis should be obtained.

## 7.0 FUNCTIONAL REQUIREMENTS

### 7.1 General

The operator should be considered as one part of an integrated system that is necessary for the proper and efficient operation of a nuclear power plant. The system shall be designed so that the operator can monitor the status of the plant and take actions necessary to control the plant.

should??

### 7.2 Display Facilities

In support of the operator needs, the control room designer should arrange the display facilities so that the operator can readily observe the displays and analyze the status of any system.

system?

7.2.1 Availability: As appropriate, the operator should have information and controls available on a "dedicated," "intermittent - periodic" or "intermittent - as called for" basis. The need for information to be displayed and its availability to the operator depends on: (1) the consequence of the operator not taking corrective action, (2) the importance of the data to the operator in determining the plant status, (3) the degree of automation to be used in control room design and (4) the use of such display techniques as "display by exception."

7.2.2 Readability and Comprehension: The display equipment should provide means to facilitate operator comprehension. These include consistent use of the following: (i) Physical differentiation of data which is presented, using such techniques as color coding, size, shape; (ii) Formats keyed to and consistent with the physical representation should be used, e.g., a vertical bar indicator



for level (iii) Graphic displays for flow diagrams, electric one lines, bar charts, etc.

7.2.3 Abnormal Conditions: The operator should be alerted to abnormal or unsafe conditions or significant changes in the plant, its process systems and/or safety systems.

7.2.3.1 Alarms - The alarm function should not be restricted solely to deviations of measured variables beyond specific limits, but rather should be, to the greatest extent possible, based on a true abnormal condition or indicated action (e.g., low oil pressure on a shaft driven oil pump on a condensate booster pump should be alarmed only when the booster pump is in service).

7.2.3.2 System Modes -- Continuous or automatic display of information, including alarms, should be safely terminated or suppressed during modes of operation when it would be meaningless, due to changes in the operating mode (such as startup, power operation, shutdown, etc.) so that information priority for the current mode of operation can be readily assessed.

7.2.3.3 Limit Monitoring - In addition to normal equipment protective limits, plant operational limits imposed by governmental agencies and by plant administrative procedures must be monitored by the operator. Provisions must be made to facilitate these requirements.

the implementation of these

should this not be systems?? a device as a unit in an electrical system which is intended to carry but not utilize electric energy - i.e. switches, breakers, relays, displays, etc. NEC P.70-7.

7.3 Control Facilities

The operator requires control devices that enable him to take the actions as dictated by plant or system needs. This includes manual control during certain phases of plant operation.

(Note: Plant operating procedures specifying operator response to alarms will be readily available to the operator.)

7.4 Device and Display Identification

Identification of control and display functions should be easily associated with the physical devices being monitored or controlled. Where alpha numeric identification systems are used, they should be supplementary to a narrative description.

7.5 Convention for Control Devices

A convention shall be established to provide consistency in the operation of controls that perform similar functions, e.g., control switches are to be turned clockwise to 'close.'

7.6 Display and Control Facilities - Special

Special requirements such as Safety Surveillance, Post Accident Monitoring and Remote Shutdown shall be considered in usage analysis described in Section 6.

7.6.1 Safety System Status: The operator should be automatically informed by means of a display system of the bypass or deliberately induced inoperability of systems which could affect the safety status of the plant. This system

see attached letter

POOR ORIGINAL

509 267

see attached letter

will be used to enhance the normal plant administrative procedures. Automatic indication of the bypass at the system level or deliberately induced inoperability of the protection system shall be provided. The indication system should also be activated by the bypass or deliberately induced inoperability of any auxiliary or supporting system, which effectively bypasses or renders inoperable the protection system or system actuated or controlled by the protection system. Each system level indicator (or indication) of the display system shall be capable of manual initiation from the central control room. This display should be used for those protection systems for which the act of bypassing or being rendered inoperative occur more than once a year.

needs clarity

In accordance with the general requirement (see Section 7.2.3.2) that the operator not be subject to confusing information. The display should only be activated when the protection system or component is expected to be available.

7.6.2 Redundant Display Information: The operator's ability to reliably interpret information will be affected by the availability of alternative sources of confirming information. Certain information pertaining to safety related systems must be readily available in redundant form such that the operator can rapidly verify the existence of an unsafe condition or trend. These alternate sources of confirming information can be in the form of redundant (i.e., two pressure alarms) or diversified (i.e., one breaker tripped alarm and one low pressure alarm or indication) information. To ensure that the operator uses both sources of information to reliably interpret the information, the devices should have the same importance.

I am not sure whether this is a viable alternative. If one pressure alarm says no pressure and the other says normal the operator is confused with conflicting information. Obviously he will have to investigate to find the true situation. Truly confirming info would be 2 out of 3 press. alarms

POOR ORIGINAL

509 268

### 7.7 Area Arrangement

The Normal Operations area should be centrally arranged within the control room to provide the operator with surveillance and access capability to other operating areas within the control room. The Emergency Operations area should be readily accessible and visible from the normal operations area. This area should not be in a separate room or enclosure from the Normal Operations area.

### 7.3 Device Arrangement

Individual devices or groups of individual devices should be arranged to minimize operator motion including changes in direction of vision.

### 7.9 Equipment or System Status

Consideration should be given to provide indication when non-safety related is taken out of service for maintenance, calibration, inspection and when it is returned to service.

### 7.10 Communications

Reliable means of communication between the operator and various internal and external bodies, such as plant security, are required. The methods provided shall not divert the operator from his principal duties.

*should?*

### 7.11 Internal Security

Where display and alarm devices are provided within the central control room to alert the operator to unauthorized entry into

vital areas, the devices should be clearly differentiated from any devices provided for plant functions by color, arrangement or location.

Tony: If you feel the above is adequate - leave it. But if you feel that the latter part of it could be improved then perhaps you might consider one of the alternatives below.

7.11. Where display and alarm devices are provided within the central control room to alert the operator to unauthorized entry into vital areas, such devices should be clearly differentiated from those used for other plant functions unrelated to security. Differentiation could be provided by the use of color, sound, arrangement or location.

7.11 Where display and alarm devices are provided within the central control room to alert the operator to unauthorized entry into vital areas such devices should be clearly distinguished from all other devices not related to security. Such devices could be clearly distinguished by the selection of color, sound, arrangement or location.

7.11. Where the central control room is provided with display and alarm devices for alerting the operator to unauthorized entry into vital areas, such devices should be clearly distinguishable from all other devices not related to security. To distinguish between security and non-security devices consideration should be given to the proper application of color, sound, arrangement or location.

POOR ORIGINAL

Example of Systems and Subsystems Analysis

- 16 509 271

23

TABLE I SYSTEM-SUBSYSTEM-COMPONENT USAGE ANALYSIS

MAJOR EVALUATION CRITERIA (1)	Plant Operating Mode When System Is Used										When Used Its Need/Act'y Is				Response			Classification			Conclusion/Ass'g't						
	Normal Operation						Emergency				Refueling	Frequent	Infrequent	Fast/Short	Slow/Long	Critical to Continuous Operation	Class I/E	Other Safety-Related	Non-safety	Norm. Oper. Pos'n		Auxiliary-Supporting Position	Emergency Position	Other Location (Local)	Auxiliary C.R.		
	Plant Start-up	Hot Start	Base Load Or Auto Load Follow	Manual Load Change	Hot Shut Down	Plant Shut Down	Accident	Post-Accident	Frequent	Infrequent										Fast/Short	Slow/Long					Critical to Continuous Operation	Class I/E
ELECTRICAL																											
Switchyard	X						X					X		X			✓										
Station Aux. Power	X	X			X	X						X		X			✓										
Diesel Gen.							X					X		X			✓										
TURBINE - GENERATOR																											
Exc Control	X	X	X	X							X			X			✓										
Tube Oil	X				X							X		X													
Hydraulic Oil	X											X		X													
Seal Seal & Drains	X				X							X		X													
Turning Gear	X				X							X		X													
Supervisory	X	X			X							X		X													
Gen. Excitation	X	X			X							X		X			✓										
Sync. Controls	X	X			X							X		X													
Gen. Seal Oil	X				X							X		X													
Gen. Hydrogen	X				X							X		X													
Stator Cooling	X				X							X		X													
MAIN STEAM																											
By-pass to Cond.																											
Steam Drains																											

SAMPLE

Information Displayed

- System Status - Normal
- System Status - Alarm
- Component Status - Normal
- Component Status - Alarm
- System Availability
- Component Availability
- Operating Parameter Display
- Limit Monitoring
- Post Accident Monitoring
- Response to Oper. Reg. for Info
- Operator Action guidance

Consequence of Action (Alarms or Control)

- Safety
- Plant Shutdown
- System Shutdown
- Start-Standby
- Minor Consequence
- None

NOTE: THIS TABLE IS TYPICAL.

X usage by the operator

✓ major evaluation criteria

More than a "sensory overload (sight & hearing) but will require assimilation of information through sight & hearing plus physical acts of manipulating controls (pressing buttons, turning switches etc).

APPENDIX

over-burden

Example of Operator Sensory Overload in Operation of Safety Systems

acting -

An operator's performance cannot be accurately predicted particularly when working under stress. The operation of the plant protection systems must therefore for the most part be independent of operator-initiated action during upset conditions. On the other hand, the memory, reasoning and decision-making capability of the operator should be utilized to the maximum extent possible to augment plant operation.

Examples of required simultaneous operator manual action during a plant incident condition in a FWR could be as envisioned below. Even though a conservative analysis indicated tolerability of the worst possible sequence of events, the actual sequence might proceed in an unforeseen way.

- 1) Selection of mode of operation of high or low pressure ECCS pumps
- 2) Reduction of diesel load
- 3) Routing of residual heat removal system to the containment building spray headers.
- 4) Switchover from ECCS water tank to reactor containment building sump in event of failure of automatic switchover.
- 5) Control rod manipulation
- 6) Restoring spent fuel cooling

generally 20-40 mins at the most hours after incident

POOR ORIGINAL

\* in the past W has gotten away with manual switchover but in recent times NRC has insisted on automatic switchover or transfer. Therefore it will be preferable to odd that manual transfer occurs only in event of failure of the automatic transfer or switchover.

509 272

Minimum 7 days  
after incident.

- 7) Replenishment of diesel fuel and makeup of cooling water
- 8) Start H<sub>2</sub> Recombiner System 5-15 days depending on severity  
of H<sub>2</sub> generation.
- 9) Start containment building air purification and cleanup
- 10) Auxiliary feedpump suction transfer.

suction?

See extensive comments in attached  
letter.

POCR ORIGINAL

509 273