AUG 29 1984

Docket No. 50 458

Mr. William J. Cahill, Jr.
Senior Vice President
River Bend Nuclear Group
Gulf States Utilities Company
Post Office Box 2951
Beaumont, Texas 77704
ATTN: Mr. J. E. Booker

Dear Mr. Cahill:

SUBJECT: BYPASSED AND INOPERABLE STATUS INDICATION FOR NUCLEAR POWER PLANT SAFETY SYSTEMS

The requirement for providing control room indication of the bypassed or (deliberately induced) inoperable status of redundant portions of safety-related systems is given in section 4.13 of IEEE Standard 279. Guidance for the design of acceptable bypassed and inoperable status indication systems is provided in Regulatory Guide 1.47 and NUREG/CR-3621 (Safety System Status Monitoring).

The bypassed and inoperable status indication system design remains as an outstanding issue in Chapter 7 (Instrumentation and Controls) of the River Bend Station Safety Evaluation Report (SER) (NUREG-0989). To further document staff concerns regarding this issue for plant safety systems at River Bend Station and to provide further guidance regarding the minimum requirements for an acceptable design, the staff has prepared the information in the Enclosure.

Please contact NRC Project Manager Edward Weinkam for further discussion on this topic.

Sincerely,

A. Schwencer, Chief
Licensing Branch #2
Division of Licensing

Distribution:
Docket File
NRC PDR
Local PDR
PRC System
NSIC
LB#2 Reading
PShuttleworth
EWeinkam
LDewey, OELD
ACRS (16)
EJordan
NGrace
RKendall

8409050618 840829
PDR ADOCK 05000458
E PDR

Enclosure: As stated

cc: See next page

OFFICE	LB#2/DL/PM	LB#2/DL/LA	LB#2/DL/BC				
SURNAME	EWeinkam/lb	PShuttleworth	ASchwencer				
DATE	8/24/84	8/ /84	8/29/84				

NRC FORM 318 (10-80) NRCM 0240 OFFICIAL RECORD COPY ☆ U.S. GPO 1983—400-247

Mr. William J. Cahill, Jr.
Senior Vice President
River Bend Nuclear Group
Gulf States Utilities Company
Post Office Box 2951
Beaumont, Texas 77704
ATTN: Mr. J. E. Booker

cc: Troy B. Conner, Jr., Esq.
Conner and Wetterhahn
1747 Pennsylvania Avenue, N. W.
Washington, D.C. 20006

Mr. William J. Reed, Jr.
Director - Nuclear Licensing
Gulf States Utilities Company
Post Office Box 2951
Beaumont, Texas 77704

H. Anne Plettinger
712 Carol Marie Drive
Baton Rouge, Louisiana 70806

Richard M. Troy, Jr., Esq.
Assistant Attorney General in Charge
State of Louisiana Department of Justice
234 Loyola Avenue
New Orleans, Louisiana, 70112

Dwight D. Chamberlain
Resident Inspector
Post Office Box 1051
St. Francisville, Louisiana 70775

Gretchen R. Rothschild
Louisianians for Safe Energy, Inc.
1659 Glenmore Avenue
Baton Rouge, Louisiana 70775

James W. Pierce, Jr., Esq.
P. O. Box 23571
Baton Rouge, Louisiana 70893

Ms. Linda B. Watkins/Mr. Steven Irving
Attorney at Law
355 Napoleon Street
Baton Rouge, Louisiana 70802

Mr. David Zaloudek
Nuclear Energy Division
Louisiana Department of
Environmental Quality
Post Office Box 14690
Baton Rouge, Louisiana 70898

Mr. J. David McNeill, III
Assistant Attorney General,
State of Louisiana
Department of Justice
Lands & National Resources Division
7434 Perkins Road
Baton Rouge, Louisiana 70808

The major staff concern with the existing design, as described in SER Section 7.5.2.2, is that system level bypassed and inoperable status indication is not provided for certain safety related systems when essential auxiliary or supporting systems (that must be operable for the safety related systems to perform their safety functions) are bypassed or rendered inoperable. Specific examples of this situation involving the diesel generators (DGs) and standby service water system (SSWS) are given in Section 7.5.2.2. Several aspects regarding bypassed and inoperable status indication designs are discussed below in order to clarify issues raised by GSU during the review, and to provide GSU with a better understanding of the staff's position regarding acceptable designs for systems used by the operators to monitor the status of plant safety systems.

o R.G. 1.47 indicates that it may not be necessary to provide automatic indication of a bypassed or inoperable status condition if the condition is not expected to occur more frequently than once per year. Bypassed and inoperable conditions include those where the capability of a redundant portion of a safety related system to perform its protective action is degraded in order to perform periodic tests or other required surveillance, including surveillance of essential auxiliary/supporting systems. Therefore, automatic bypassed and inoperable status indication (or degraded status indication, if appropriate) should be provided for any safety related system whose protective action is negated (i.e., is not operable in accordance with Technical Specifications) more frequently

than once per year in order to perform periodic surveillance.

- A safety related system is not considered to be operable if the system is dependent on backup non-safety related auxiliary or supporting equipment/systems to perform its protective action. For example, a diesel generator is not considered to be operable if the associated safety related standby service water train is inoperable, although the non-safety related normal service water system may be available to provide cooling water to the diesel generator. This is consistent with the BWR Standard Technical Specification definition of OPERABILITY:

> A system, subsystem, train, component or device shall be OPERABLE or have OPERABILITY when it is capable of performing its specified function(s) and when all necessary attendant instrumentation, controls, electrical power, cooling or seal water, lubrication or other auxiliary equipment that are required for the system, subsystem, train, component or device to perform its function(s) are also capable of performing their related support function(s)

Credit may not be taken for non-safety related equipment to function to mitigate the consequences of accidents. This is consistent with the FSAR Chapter 15 accident analyses. Therefore, if a safety related system is dependent on non-safety related auxiliary or supporting equipment to accomplish its protective action (due to the bypassed or inoperable condition of a safety related auxiliary or supporting system), then the degraded status of the safety related system should be continuously indicated in the control room.

- The staff agrees with GSU that a safety related system may be able to perform its function although it relies on a non-safety related auxiliary or supporting system. The staff also agrees with GSU that it is desirable to distinguish between the inoperability of safety systems (i.e., where a system is unable to perform its safety function) and degraded status conditions (i.e., where a system is dependent on non-safety related auxiliary/supporting systems to perform its safety function). Continuous indication of any degraded or inoperable status condition of a safety related system must be provided in the control room so that the operator(s) can make knowledgeable decisions regarding its availability to respond to accident conditions (which include the loss of offsite power). Therefore, it is important to incorporate good human engineering principles into the design of the bypassed and inoperable (or degraded) status indication system. Guidance for designs using good human engineering principles in this area is provided in NUREG-0700 (Guidelines for Control Room Design Reviews), NUREG/CR-3217 (Near-Term Improvements for Nuclear Power Plant Control Room Annunciator Systems), and NUREG/CR-3621.

- Bypassed and inoperable status indication (or degraded status indication) should be provided at the system level when any essential auxiliary or supporting system required for the safety related system to operate is bypassed or rendered inoperable, even if the

auxiliary or supporting system is a safety related system itself. This applies regardless of the fact that the safety related auxiliary/supporting system has its own system level bypassed and inoperable status indication, and is consistent with Regulatory Position C2 of R.G. 1.47.

- The use of manually actuated safety system status monitoring systems has been judged by the staff to be very susceptible to human errors. This is summarized in Appendix A to NUREG/CR-3621. Manually performed tasks that involve the updating of safety system status boards, verification of operability of redundant safety systems, and verification of the status of safety related equipment (during all modes of operation), have been judged to be highly important tasks (in terms of plant safety) that are significantly prone to human errors (i.e., the associated human error rating factor is high). For these reasons, the staff requires that automatic bypassed and inoperable status indication (using the Standard Technical Specification definition of operability) be provided in the control room for those conditions listed under Regulatory Position C3 of R.G. 1.47.

Section 4 (System Acceptance Criteria) of NUREG/CR-3621 defines the acceptance criteria which ensure that a system designed to monitor the status of plant safety systems, will effectively aid the control room operator(s) in this task. These acceptance criteria are provided in Attachment 2. As stated during the June 18, 1984 meeting, a safety system status monitoring design that complies with the acceptance

criteria is acceptable from a human factors point of view. The staff believes that in order to satisfy the acceptance criteria, automatic system level indication in accordance with Regulatory Position C2 of R.G. 1.47 is required. The staff recognizes that automatic indication of all bypassed and deliberately induced inoperable status conditions of safety related systems is not practicable or cost effective. In these cases, manual actuation of the system level inoperable status indicator, and functional testing that demonstrates system operability prior to its return to service may be sufficient.

The River Bend control room design includes a system level inoperable status annunciator point for each safety related ESF system. Beneath the associated annunciator point, each of these systems has a component/subsystem inoperable/bypass status indication display (i.e., an "eggcrate" display) that provides more specific information regarding the inoperable status condition. The individual status lights that make up this display (with the exception of the manual inoperable status activation switch) are hardwired and cannot be manually actuated. It is our understanding that these eggcrate displays contain spare status lights which GSU may elect to use to provide indication of the degraded status of safety related systems when associated safety related auxiliary/supporting systems are bypassed or rendered inoperative. We further understand that GSU would manually initiate this indication in accordance with alarm response procedures to be followed upon receipt of system level inoperable status annunciation for the auxiliary/supporting system. Actuation of the added degraded status condition lights would

not actuate the associated system level inoperable status annunciator points.

The staff believes that a design modification as described above offers several desirable features not included in the existing design. However, the staff remains concerned that the added degraded status indication would not be automatically actuated when the associated auxiliary/supporting system is bypassed or rendered inoperable. The staff's position is that automatic indication in accordance with Regulatory Position C2 of R.G. 1.47 is necessary to prevent human errors inherent in the use of manually actuated safety system status monitoring designs. In addition, an automatic status indication design would prevent the operator(s) from having to follow additional procedures. It appears to the staff that a degraded status indication design such as the one described above, but automatically actuated, would be of significant value in terms of the safety benefit gained, and would not require extensive logic or control board wiring modifications.

Personnel errors resulting in the inoperability of safety related systems have occurred at an excessive rate during the past several years. Systems are being incorrectly removed from service, or returned to service when they are not operable. These errors have occurred despite requirements (NUREG-0737; TMI Action Plan Item I.C.6) that plant procedures include provisions for independent verification of the status of safety related system components. These errors have often been attributed to inadequate procedures, the failure of plant personnel to follow procedures, or the lack of continuous awareness of the status of

safety related components by shift supervisors and operators. The following IE Information Notices address these concerns:

1. IE INFORMATION NOTICE NO. 84-37: USE OF LIFTED LEADS AND JUMPERS DURING MAINTENANCE OR SURVEILLANCE TESTING (dated May 10, 1984)

2. IE INFORMATION NOTICE NO. 84-42: EQUIPMENT AVAILABILITY FOR CONDITIONS DURING OUTAGES NOT COVERED BY TECHNICAL SPECIFICATIONS (dated June 5, 1984)

3. IE INFORMATION NOTICE NO. 84-51: INDEPENDENT VERIFICATION (dated June 26, 1984)

4. IE INFORMATION NOTICE NO. 84-58: INADVERTENT DEFEAT OF SAFETY FUNCTION CAUSED BY HUMAN ERROR INVOLVING WRONG UNIT, WRONG TRAIN, OR WRONG SYSTEM (dated July 25, 1984)

7.5.2.2 Bypassed and Inoperable Status Indication

The design of the automatically initiated ESF systems at River Bend is such that a redundant portion of certain systems may be placed in an inoperable status or bypassed during the performance of periodic tests or maintenance. To alert the operator(s) of the inoperable or bypassed status of plant safety systems, administrative procedures are supplemented with automatic indication of system inoperability. The automatic indication consists primarily of annunciator points (visual and audible indication) in the main control room. A separate inoperable and bypassed status panel is not provided. Typical plant conditions that actuate system inoperable annunciators are system in test, loss of control power, system valve misalignment, and system pump or breaker inoperable. Status lights (valve position and pump running) are often provided at the remote manual control switches for ESF system equipment. However, the staff does not consider equipment status lights acceptable to provide positive indication of inoperability or loss of redundancy of safety systems. The system inoperable annunciator points at River Bend can be manually actuated.

Guidance for the design of bypassed and inoperable status indication for safety systems is provided in RG 1.47. Position C.2 of RG 1.47 states that if the bypassing or deliberately induced inoperability of an auxiliary or supporting system effectively bypasses or renders inoperable a portion of the protection system, then automatic indication of the inoperable status of that portion of the protection system should be provided in the control room. Ideally, this indication should be presented so that the operator(s) can easily identify those redundant portions of safety systems that are not available.

The staff review of the inoperable and bypassed status indication at River Bend indicates that inoperable status indication for safety systems is not always provided when essential auxiliary or supporting systems are rendered inoperable. For example, the manual bypassing of one train of SSW does not cause automatic system level inoperable status indication for the associated diesel generator, RHR system train (the RHR heat exchangers are required in the shutdown cooling and suppression pool cooling modes), and ECCS trains (pump room unit coolers) that require SSW for cooling. Similarly, if an emergency diesel generator is removed from service, inoperable status indication for the ESF systems that rely on emergency power from that diesel generator is not provided.

The staff recognizes that when a particular auxiliary or supporting system is removed from service, the function performed by that system is not necessarily lost (e.g., in the cases of standby service water and the diesel generator, normal service water and offsite power may be available to accomplish these functions). However, the FSAR Chapter 15 accident analyses, which are used to demonstrate the ability of the plant to accommodate the consequences of accidents (and thus, as a basis for licensing), assume that offsite power is not available and that the mitigating (safety) systems can accomplish their safety function given a single failure. Therefore, offsite power and normal service water cannot be relied on as essential auxiliaries to safety-related equipment, and must be assumed to be unavailable. The availability of nonsafety-related auxiliary/support systems is not sufficient justification for not providing system level bypassed and inoperable status indication when safety-related auxiliary/support systems are rendered inoperable.

In accordance with Section 4.13 (Indication of Bypasses) of IEEE 279-1971, the applicant must provide inoperable status indication in the control room when the protective action of a system required for safety has been bypassed or deliberately rendered inoperative.

4.0 SYSTEM ACCEPTANCE CRITERIA

The previous section of this report concluded that procedures are effective in reducing memory errors but they are not effective in reducing all errors associated with monitoring the status of the safety systems. Although existing systems did aid the operator, no system was effective in reducing error likelihood for all of the monitoring tasks. Based upon an analysis of the problems facing the operators as they monitor the status of the safety systems, this section defines a set of functional requirements that must be met by any system designed to effectively aid the operator in this task. The section then defines the acceptance criteria for a system that will meet those functional requirements.

4.1 ASSUMPTIONS

There are three assumptions underlying the following criteria. The first assumption is that improvements can be made to the methods used to monitor the status of the safety systems. The second assumption is that it is impractical to retrofit instrumentation to all of the non-instrumented components. The third assumption is that even if the plant installs an automated system, procedures will be used to some extent in monitoring the status of the safety systems.

4.2 FUNCTIONAL REQUIREMENTS

The goal of any system that monitors the status of the safety systems is to provide current and accurate status information, and to reduce the likelihood of error in all of the error-susceptible tasks involved. Previous sections of this report identified those tasks with a high likelihood of error and those that were judged to be important. Based on these results, four basic functional requirements were derived. These requirements should be met by any system that is used to monitor the status of the safety systems:

- The system should minimize the operators' need to search for task-relevant information. The operator should have access to needed information without having to sift through irrelevant inputs or to obtain information from diverse locations.

- The system should facilitate component identification and minimize encoding errors. Errors in encoding arise from failures to sense information or from miscomprehension of sensed information. The data should be presented in a way that reduces the probability of misperception or misinterpretation. Illegible or ambiguous information increases the likelihood of errors in encoding. Similarly, incomplete, inaccurate, unreliable, or noisy information also degrades encoding.

- The system should simplify the information processing tasks. There are two basic types of information processing tasks. The first is comparison tasks that may involve comparisons between various items of remembered information (mental comparison), written or spoken information (sensory comparison), or a combination of mental and sensory sources. Examples of these tasks are comparing one list of valves for correspondence with another, and comparing a maintenance request sheet with a maintenance tag. The second type of information processing tasks is those that involve complex reasoning steps. These tasks are especially susceptible to error. Examples of these tasks include determining system status based on component status data and determining the effect that the removal of a component will have on the system.

- The system should minimize the need for the operator to rely on memory. Humans have a limited capacity to pick up and store information. Errors in information storage include failing to store information and storing incorrect information. Similarly, errors in retrieval include forgetting and misremembering previously stored information.

These functional requirements describe in a general way the human interface considerations that should be addressed by a man-machine system designed to monitor the status of safety systems. Presented below are a set of acceptance criteria to help in evaluating a system to determine how well it meets the aforementioned functional requirements.

4.3 ACCEPTANCE CRITERIA

In order to ensure that a system meets the functional requirements defined above, the following set of acceptance criteria should be met:

1. A means should be provided to determine and display the status of each safety system during all modes of operation. The system should indicate at the system level the bypass or deliberately induced inoperability of the safety system. For those systems with redundant trains, the system indication should be by train. The display should emphasize the effects that bypassing a component has on safety systems rather than the effects on auxiliary or supporting systems. The determination of system and availability should include non-instrumented as well as instrumented components.

2. A means should be provided to determine the status of each individual component within a safety system. Component status need not be displayed at all times. However, if a safety system is bypassed or inoperable, the operator should be able to quickly and reliably identify which individual component or components are bypassed or inoperable. The determination of component availability should include non-instrumented as well as instrumented components.

3. A means should be provided to easily identify all of the components of each safety system and those components in auxiliary or supporting systems that must be operable for safety systems to perform their function. The operator should be able to obtain this listing (or other type of display) by providing safety system identification. This listing should show the current status of each component if the operator requires that information. The non-instrumented components should be included.

4. A means should be provided to identify the system or systems of which any component is a part. The operator should be able to obtain this information by providing component identification.

5. A means should be provided to determine how the removal of a component or components affects a safety system or systems. Once the operator identifies the component(s), the system should then aid the operator in determining what effect the removal of the component(s) would have on the safety systems. Effects that are dependent on changes in plant mode should be included. The system should aid the operator in recognizing the effects of bypassing both: 1) components within safety-related systems or trains; and 2) any component of an auxiliary or support system that has the potential to degrade or make a safety system inoperable.

6. A means should be provided to ensure that all information on component or system status is valid, reliable, and timely. Changes in component status should be updated and communicated to control room operators as soon as possible. This criterion is extremely important for non-instrumented components.

7. A means should be provided to ensure positive identification of non-instrumented components. The system should aid the operator in identifying the correct component during the manual verification of its status.

8. A means should be provided to ensure positive identification of the status of the components.

9. The system should provide ready access to relevant engineering information (e.g., P&ID's, E-Prints, and other technical data) in a simple and understandable format.

10. Displays should be designed for operator use and should contain only information relevant to the operator's task. The operator should not have to sift through irrelevant information.

11. Whenever procedures are used as part of the system, they should be tailored to the specific task type and should be written using a recognized procedures writing guide that incorporates both human factors and effective communications principles.

12. Systems for monitoring safety systems status should follow accepted human factors standards and practices. These standards and practices should be applied to hardware, procedures, and training, as well as software, if a computer-based system is used.

A system that is designed to meet these acceptance criteria should reduce the likelihood of error associated with the tasks that occur in monitoring the status of the safety systems.