DP-MS-80-100

# AUTOMATIC DIAGNOSIS OF ALARMS, A SYSTEM TO IMPROVE OPERATOR EMERGENCY RESPONSE

by

H. P. Olson, K. L. Gimmy, E. Nomm, and R. H. Finley

E. I. du Pont de Nemours & Co.
Savannah River Laboratory
Aiken, SC 29808



Proposed for presentation at the International Conference on Current Nuclear Power Plant Safety Issues, October 20-24, Stockholm, Sweden and for publication in the proceedings.

---

INTERNATIONAL ATOMIC ENERGY AGENCY

**INTERNATIONAL CONFERENCE ON CURRENT NUCLEAR POWER PLANT SAFETY ISSUES**

Stockholm, 20—24 October 1980

**IAEA-CN-39/** 96

# AUTOMATIC DIAGNOSIS OF ALARMS: A SYSTEM TO IMPROVE OPERATOR EMERGENCY RESPONSE

H. P. OLSON, K. L. GIMMY, E. NOMM, AND R. H. FINLEY
E. I. du Pont de Nemours and Company, Savannah River Laboratory, Aiken, South Carolina 29808 USA

# AUTOMATIC DIAGNOSIS OF ALARMS: A SYSTEM TO IMPROVE OPERATOR EMERGENCY RESPONSE


## ABSTRACT

A system is being developed at the Savannah River Plant to help reactor operators respond to multiple alarms in a developing incident situation. The need for such systems has become evident in recent years, particularly after the Three Mile Island incident.


## INTRODUCTION

### Savannah River Reactors

The Du Pont Company operates three reactors at the Savannah River Plant (SRP) to produce nuclear materials for the U. S. Department of Energy. The reactors are moderated and cooled with low pressure heavy water, and are operated at 2000 to 2500 MWT using ordinary water as a heat sink (Figure 1). These reactors have been operated for 25 years.

Online computers for monitoring reactors were first installed in 1964. Each reactor now has four computers for monitoring, control, and safety functions (Figure 2). Two of the computers (safety computers) rapidly scan flow and temperature signals from each of the 600 reactor fuel assemblies and are able to scram the reactor if prescribed set points are exceeded [1]. Two other computers (control computers) monitor signals from 2400 thermocouples and 250 other sensors and normally move control rods to adjust reactor power and power distribution. The control computer system was updated in 1977 when the safety computers were installed.

Overall, SRP has about 30 reactor-years of experience with closed-loop computer control [2]. Computer operating experience has been excellent. Both safety computers are online and unbypassed about 98% of the time. The dual-control computer system

with input/output bus switching has a demonstrated innage of 99% for essential functions. The control computer system was designed to be expanded to handle an alarm-pattern diagnosis function.

**The Need for Automatic Diagnosis of Alarms**

A high priority effort is under way to improve operator response to alarm annunciators. As with most large nuclear reactors, the control room for SRP reactors contains many alarm plates (back lighted messages) to announce abnormal conditions. A typical panel is shown in Figure 3. Operators respond to these alarms according to written procedures. The alarms are grouped according to major systems (such as primary cooling system, secondary cooling system, and helium gas system). The alarms within each group are assigned a priority number. Operators are trained to respond to the highest priority alarm within a group. Alarm priorities among the groups have not been prescribed.

Minor incidents typically involve one alarm plate. The operator is able to respond to a single-alarm with no difficulty. He obtains the procedure corresponding to the alarm that is on and takes the prescribed action. At the other end of the accident spectrum, a very serious accident, such as a major loss of primary coolant, would be handled by automatic actuation of emergency cooling; or in some cases a special annunciator directs the operator to actuate the emergency cooling system. Between these two extremes is a broad area of possible conditions where the operator could be confronted by many alarms, some of which could be extraneous. Even an experienced and well trained operator could have difficulty analyzing the situation. If he is unable to diagnose and correct the problem, the situation may deteriorate and bring even more alarms, adding to the difficulty. It is in this area of multiple alarm situations that the operator needs assistance.

**SUMMARY**

A system is being developed at the Savannah River Plant to assist reactor operators in their response to developing incident or accident situations. The system, called the "Automatic Diagnosis of Alarms" (ADA), will use existing control computers to analyze the pattern of alarms that would accompany a leak from the primary or secondary cooling system.

The computer will provide a message on a video display unit that will indicate the type and location of the leak and other pertinent information. The system will not take action, it will only advise the operator. The system can be expanded to include other types of accidents. This first step, analysis of leaks, is an area where operator assistance is most needed. The initial installation will use about 60 existing alarm annunciators and 20 process signals.

The logic for the system will be stored in a computer memory as a decision table, which will be processed by the ADA program whenever an alarm changes state. This method of storing the logic has several advantages. The table can be expanded easily without changing the softwear that processes the table, and the table can be audited easily by the method of checksums. These advantages are important, because we anticipate revisions and growth. The logic from about 40 alarm trees is now being coded, and off-line auditing programs are being developed to check out the software. The first ADA system will be operable in mid 1981.

**DISCUSSION**

**The Automatic Diagnosis of Alarms (ADA) System**

The ADA system that SRP is developing will be a limited first step to assist the operators diagnose the cause of multiple alarms. It will be limited to locating leaks in the primary and secondary cooling systems. The goal is to identify the leaking portion of piping so that the leak can be isolated. This first

step in ADA development is small enough to be manageable, yet it will greatly enhance the ability to isolate medium sized leaks before they progress to the point where it becomes necessary to actuate the emergency cooling system (light water). If emergency cooling can be avoided, the heavy water will not be diluted and the release of its tritium to the environment will be minimized. Medium sized leaks are estimated to be more likely than very large leaks that require rapid automatic actuation of emergency cooling, but in the remote chance that a large pipe breaks, the ADA system will also help the operators manage that situation.

The ADA system uses the control computers to analyze the alarms that are activated by a leak. Specific patterns of alarms have been defined to help locate the leak. The computer searches for these patterns and when one is identified, an output message on a video display unit will advise the operator of the location of the leak and give him other pertinent information. The ADA system takes no control action, it only advises the operator.

The alarm patterns are being developed in the form of logic trees that are similar to relay logic diagrams. Figure 4 shows a very simple example of a tree element. Decisions in the tree are given both numbers and names that have meaning to operators. Some of these decisions have definite meanings and are called primitive decisions. For example, Decision 501 in Figure 4 is a primitive decision that is named "Leak, Primary System." Once a primitive decision is defined it can be used in subsequent tree branches without redefinition. This has advantages. First, it establishes standard conditions that are consistently applied, i.e., one and only one definition for each condition. Second, named primitive conditions make it easier for people to follow the logic, especially for quality assurance auditing of the computer software.

Combinations of decisions lead to higher order decisions that produce messages on the video display unit. The message in Figure 4 is "Leak, Primary System, Pump Room." The message from a more complicated tree might be "Leak, Primary system, Pump Room, system 6, 50 gpm." This would require in addition to the decisions of Figure 4, other inputs and decisions, and an analog

input. A complete message such as this gives the operator much of the information he needs to isolate the leak as well as an indication of how quickly he must act to avoid emergency coolant actuation.

Figure 5 shows an example of a video display. Leak location and rate information are given, as well as the procedure the operator should use to isolate the leak. The procedure will indicate the specific valve numbers and give detailed instructions. Another bit of information that is given is which closed-circuit TV cameras to monitor to help locate the leak. A closed circuit TV system is an independent leak-location system being developed as an adjunct to the ADA system. The control room radiation level and air quality information is included to advise the operator of his own personal safety.

The information shown in the example would reassure the operator and encourage him to concentrate on controlling the leak. If his personal safety is threatened by high radiation levels, the display would flash "EVACUATE." The leak rate information initially indicates the urgency of the situation. Subsequently it tells the operator if his control actions are helping. If the leak rate decreases, he has done the right thing; if not, something else must be done.

A key design feature of the ADA system is to give the decision message at the highest level possible. In some cases, because of missing alarms, this might be a lower level decision or even a primitive decision name. Any advice, if accurate, is better than none.

**Softwear Development**

All of the logic trees will be combined into a single decision table that will be programmed for the control computers. Figure 6 shows the decision table corresponding to the simple tree element of Figure 4. The table denotes the "and," "or," and "nor," logic of the trees by specifying the "m of n" condition required:

m = 1 denotes "or"

m = n denotes "and"

m = 0 denotes "nor".

Events and decisions are identified by numbers in this table, and in the softwear package. Other reference tables will contain appropriate descriptive and identifying names and messages, which are used for computer output messages that are easily understood by the operators. In the tree, primitive decisions are building blocks for higher level decisions, and therefore primitive decisions must be processed before higher order decisions. This is accomplished by the order of the elements of the decision table. The priority of output message is also established, and the highest priority messages will be displayed.

The method of storing logic as numbers in a decision table has three advantages over conventional programming subroutines. First of all the decision table is easily expandable to include new diagnostic logic. The table can be altered to add new inputs and decisions, or to modify current ones, without requiring any changes in the program that processes the table. This is an important feature, because we anticipate additional ADA logic development and growth of the ADA at SRP.

The second advantage is the ease of verifying the correctness of data entered into the control computer by method of checksums.

Third, the decision table method facilitates auditing of ADA logic. Auditing programs have been written for use on off-line computers to check for logical inconsistencies in the table, such as circular reasoning and missing, or too many, inputs to m-out-of-n decision gates. The auditing programs also provide useful cross-reference listings in easily understandable language.

We will implement ADA in the control computers in the following way. Whenever an alarm changes state (on-to-off or

off-to-on), the computer will do two things; record the new state of the alarm in its memory, and cause the ADA program to process the entire decision table to see if any combinations of alarm states exist that would produce an output of a diagnostic message. The key feature here is that the entire table is reprocessed when alarms change. This is important because of the message priority system, which will place greater importance on certain diagnostic messages over others. The idea is to generate all possible messages and then to display the most important one. All displayed messages are logged on a hard copy printer for a permanent record of events during an incident. The information flow is illustrated in figure 7.

One danger, however, is that the alarms could be changing states very rapidly due to actual process changes or equipment malfunction such as relay chatter. Such a condition could cause display messages to change too rapidly to be of value to the operator. To overcome this difficulty, the computer will check input signals for persistence and validity. For example, only signals with more than a specified duration will be accepted. Also alarms that continue to change state back and forth will be rejected as bad signals. Other spurious alarms, such as those caused by electrical power loss, will also be rejected by ADA. One important feature in alarm discrimination is that alarms will continue to light up on the existing alarm display panel. The rejection of alarms will affect only the automated computer diagnostics. The system will also include provision for manually masking alarms that are out of service for maintenance.

**Adjustment of Analysis Sensitivity**

The "m of n" logic specified in the decision table can be adjusted to alter the sensitivity of the analysis. This provides flexibility that is not possible with simple "and" - "or" decision logic. For example, an "or" decision with 3 inputs in the logic tree would initially have n = 3, m = 1 in the decision table for 1 out of 3 logic. But if one of the inputs has a history of alarming spuriously, for example, the designer might choose to alter the decision logic to 2 out of 3 to prevent invalid decisions. All that is required to accomplish this is to

change m = 1 to m = 2 in the decision table. No programming changes are required. Similarly, an "and" decision logic can be changed from 3 out of 3 to 2 out of 3, to make satisfaction of the logic more likely. Thus, the designer can "tune" the sensitivity of the decision table based on experience and judgement.

An extension of this flexibility, now being considered, would be to allow the operator to adjust, on demand, the sensitivity of the primitive decision logic. The sensitivity adjustment feature could consist of two buttons on the ADA console that the operator can use to select "more" or "less" sensitivity. The "more" button decrements "and" gates at the primitive decision level (e.g., 3-out-of-3 logic becomes 2-out-of-3), and the "less" button increments "or" gates at the primitive decision level (e.g., 1-out-of-3 logic becomes 2-out-of-3). This interaction capability has a potential to compensate for the designer's inability to predict accident sequences and alarm operability exactly. The "more" option would be useful in a situation where an incident has occurred and at the same time a random alarm failure prevents ADA from completing its diagnosis. The operator knows that something has gone wrong, but he does not get any help from ADA. By pushing the "more" button he reduces by one the number of inputs required to satisfy primitive level "and" gates. This eliminates the need for an input from the failed sensor, and ADA is able to display something useful to the operator. Similarly, the "less" option would be useful in a situation where too many alarms come on at the same time, causing several messages of almost the same priority to be registered in the message queue. By incrementing "or" gates, the operator is able to ask for greater confirmation of inputs and in that manner may be able to make one message clearly stand out above the rest. The adjustable sensitivity feature has potential utility but still needs development.

Savannah River plans to install the ADA system in the first of three reactors in mid 1981. The first installation will require about 80 inputs to the computer (both digital and analog) and will be programmed with diagnostic logic from about 40 alarm

trees related to primary and secondary cooling water systems. In summary the ADA will provide the following functions:

1. Detect and locate leaks
2. Analyze the need for manual emergency cooling water addition
3. Direct operators to the correct written procedures
4. Direct operators to proper closed circuit TV cameras
5. Display leak rates
6. Display Control Room radiation conditions

## REFERENCES

[1] GIMMY, K. L., USERDA Rep. DPSPU 77-30-3 (1977).

[2] GIMMY, K. L., Trans. Am. Nucl. Soc. 14 Suppl. 2 (1971) 31.

## ACKNOWLEDGEMENT

The information contained in this article was developed during the course of work under Contract No. DE-AC09-76SR00001 with the U.S. Department of Energy.

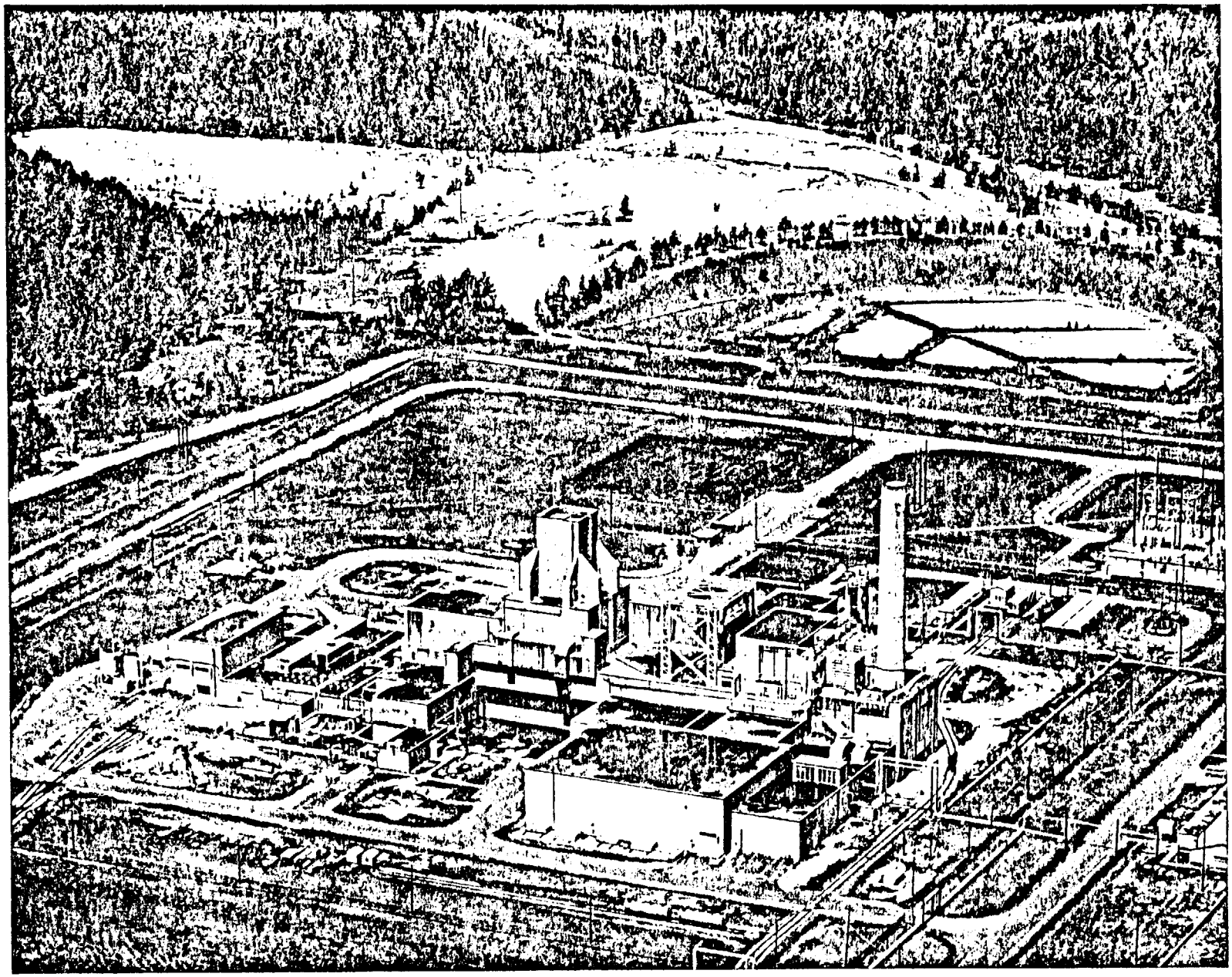


FIG. 1 Savannah River Reactor

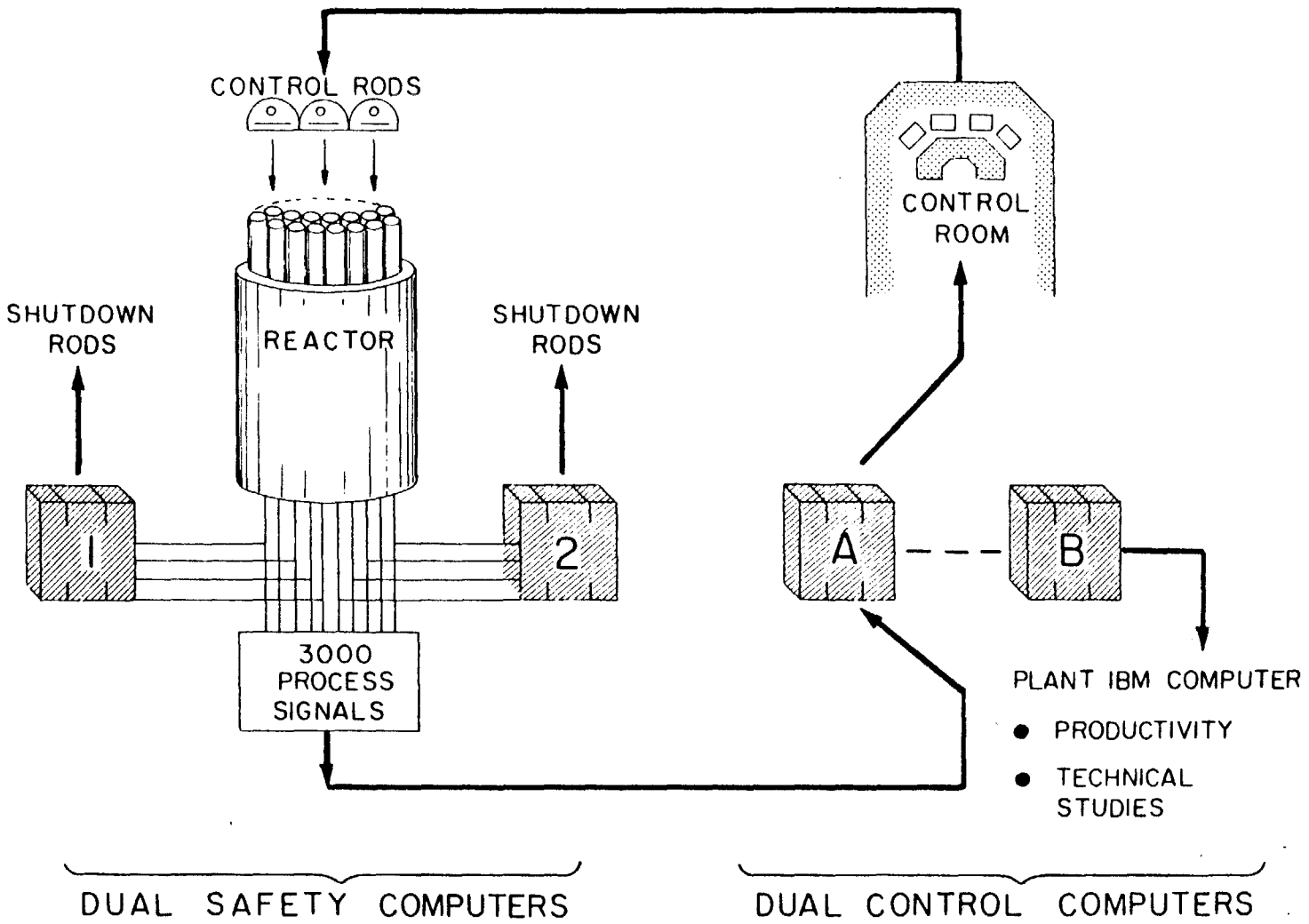



FIG. 2 Reactor Computer Systems

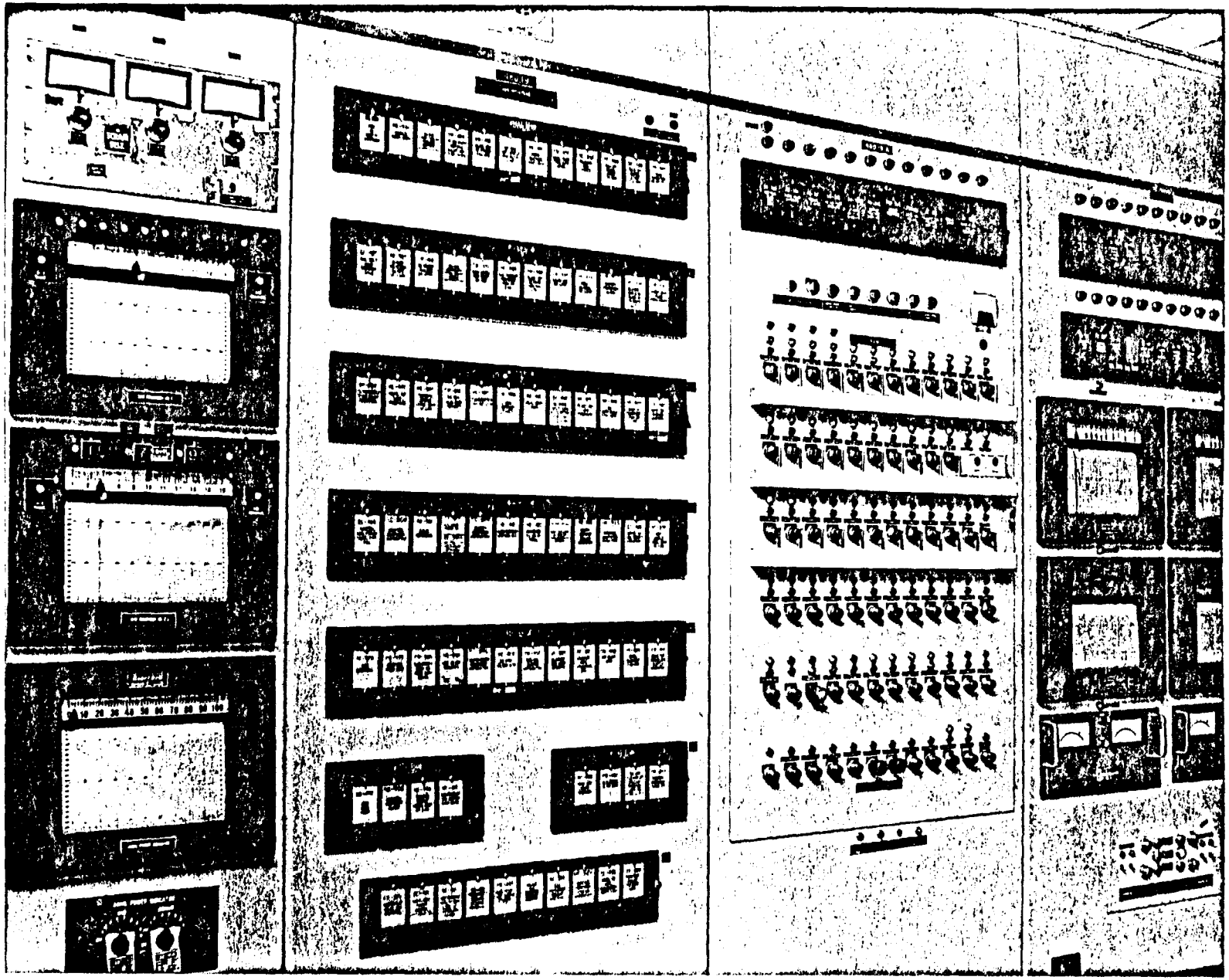


FIG. 3 Typical Annunciator Panel

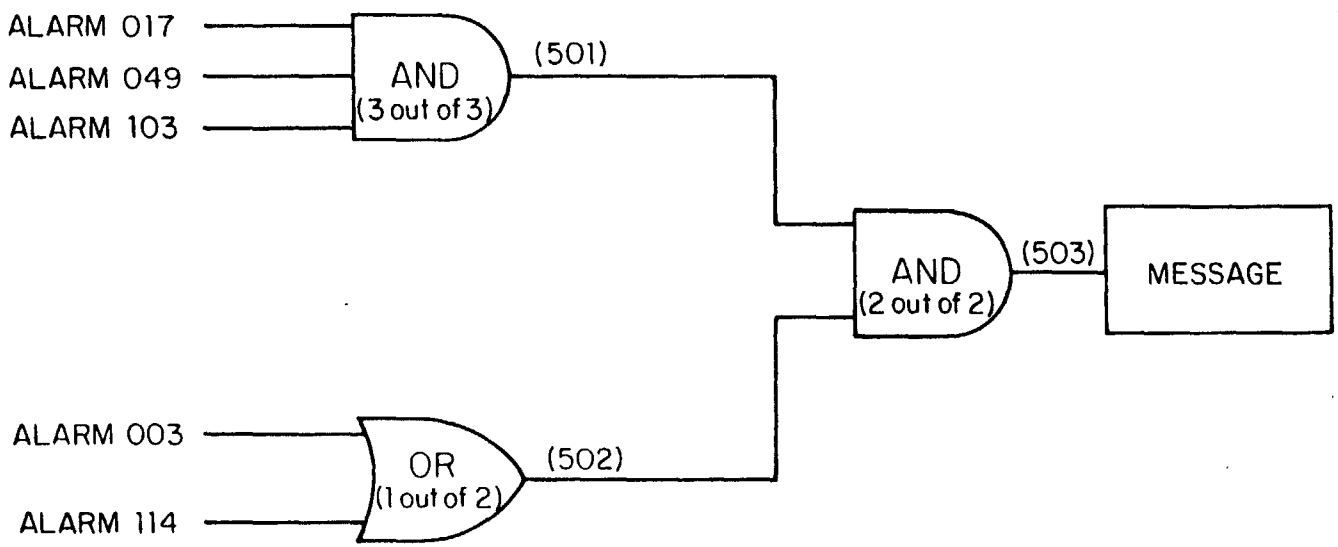



FIG. 4 Typical Logic Tree

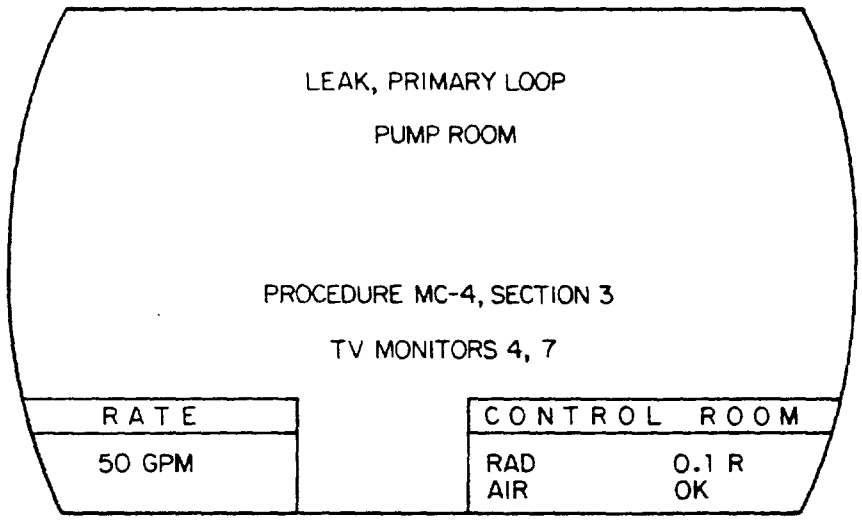
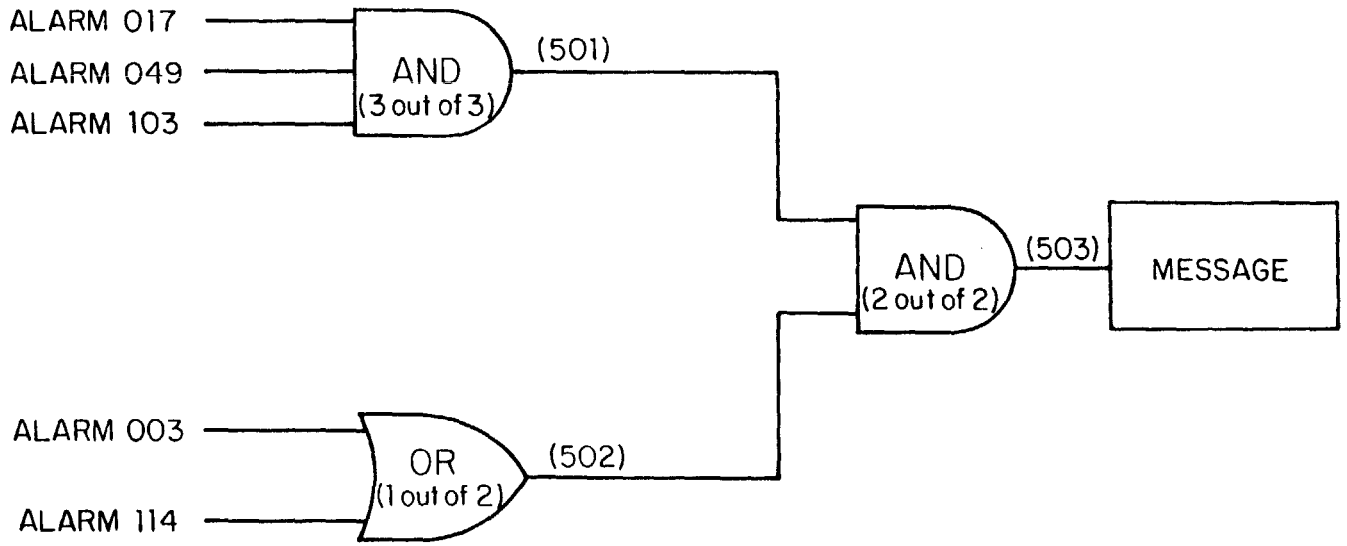



FIG. 5 Alarm Analysis Display




| Decision | Number of Inputs | Number Required | Input Identification | Message |
|---|---|---|---|---|
| 501 | 3 | 3 | 017, 049, 103 | NO |
| 502 | 2 | 1 | 003, 114 | NO |
| 503 | 2 | 2 | 501, 502 | YES |

**FIG. 6 Typical Decision Table**

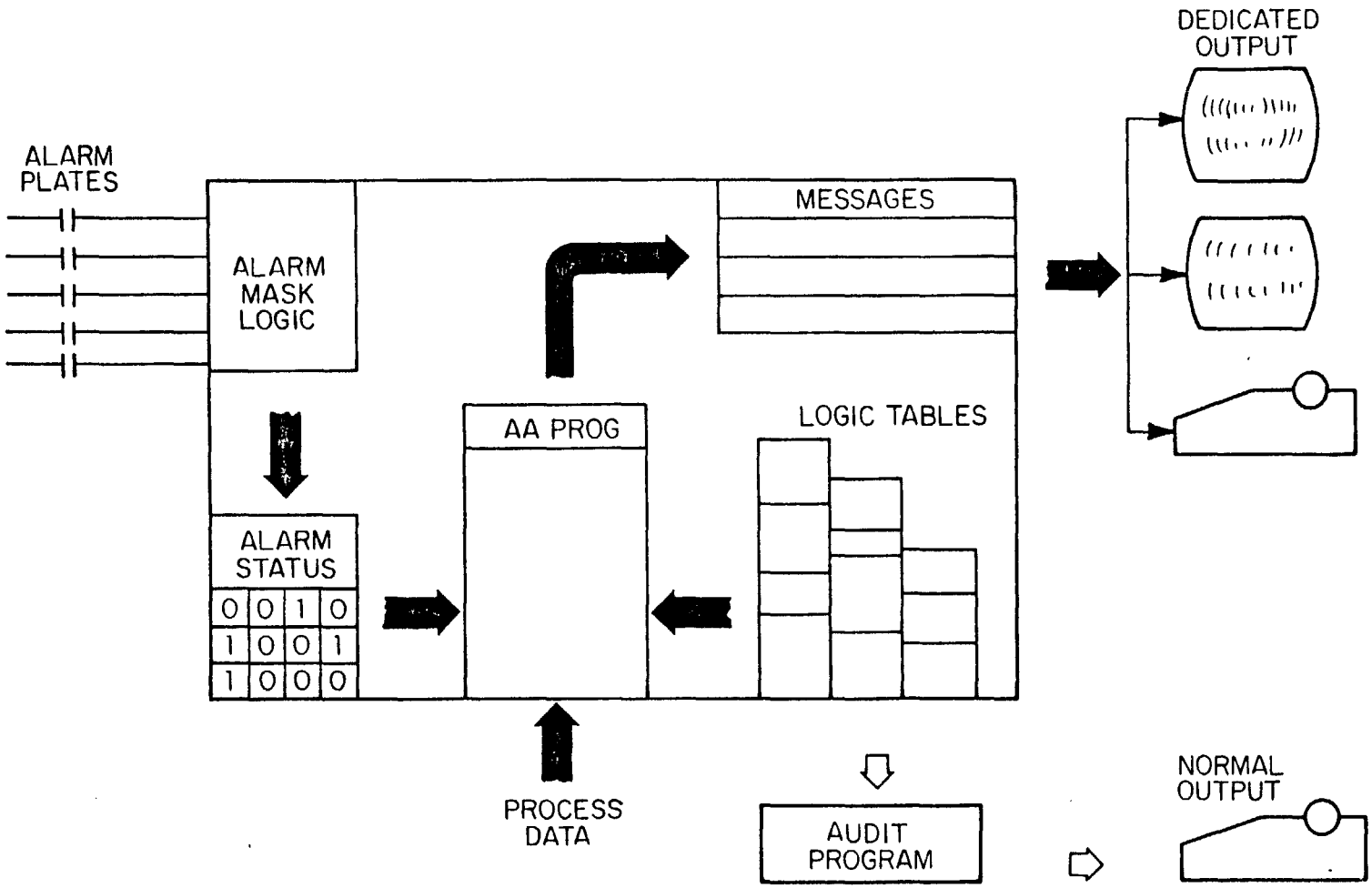



FIG. 7 Data Flow for Alarm Analysis