MARTIN MARIETTA ENERGY SYSTEMS LIBRARIES

3 4456 0325292 2

ORNL/TM-11714

ornl

OAK RIDGE
NATIONAL
LABORATORY

MARTIN MARIETTA

Single-Failure-Proof Considerations for the K-25 Site Radiation Alarm System

K. N. Castleberry

OAK RIDGE NATIONAL LABORATORY
CENTRAL RESEARCH LIBRARY
CIRCULATION SECTION
4500N ROOM 175
LIBRARY LOAN COPY
DO NOT TRANSFER TO ANOTHER PERSON
If you wish someone else to see this report, send in name with report and the library will arrange a loan.

OPERATED BY
MARTIN MARIETTA ENERGY SYSTEMS, INC.
FOR THE UNITED STATES
DEPARTMENT OF ENERGY

This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from the Office of Scientific and Technical Information, P.O. Box 62, Oak Ridge, TN 37831; prices available from (615) 576-8401, FTS 626-8401.

Available to the public from the National Technical Information Service, U.S. Department of Commerce, 5285 Port Royal Rd., Springfield, VA 22161.

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

ORNL/TM-11714

Instrumentation and Control Division

SINGLE-FAILURE-PROOF CONSIDERATIONS FOR THE K-25 SITE RADIATION ALARM SYSTEM

K. N. Castleberry

Date Published—December 1990

Prepared by the
OAK RIDGE NATIONAL LABORATORY
Oak Ridge, Tennessee 37831-6285
managed by
MARTIN MARIETTA ENERGY SYSTEMS, INC.
for the
U.S. DEPARTMENT OF ENERGY
under contract DE-AC05-84OR21400

MARTIN MARIETTA ENERGY SYSYEMS LIBRARIES

3 4456 0325292 2

CONTENTS

ABSTRACT v

1. INTRODUCTION 1

2. DOUBLE COVERAGE 3

3. SINGLE-FAILURE-PROOF CRITERIA 5

4. SYSTEM CONSIDERATIONS 7

5. CLUSTER MODIFICATIONS 9

6. FINAL COMMENTS 13

7. REFERENCES 15

ABSTRACT

The Oak Ridge K-25 Site Radiation Alarm System currently provides monitoring coverage for all areas of the plant where nuclear materials are stored or handled. This system monitors these areas with 50 instrument clusters, each comprising 3 independent radiation detection instruments. Cluster placement and radius of coverage provide double cluster coverage for most designated areas of the plant even though the clusters are redundant in themselves; the entire radiation alarm system would be single-failure-proof with inclusion of the modified cluster logic module, printed circuit board in each cluster unit assembly even without redundant coverage. It is estimated that 10 additional clusters, which are not available, will be required to provide full double coverage for all designated plant areas and to provide adequate operating spares for system maintenance activities. The removal of those clusters now providing redundant coverage would easily provide an adequate number of operating spares and eliminate the need for additional procurement.

1. INTRODUCTION

The radiation alarm system (RAS) at the K-25 Site (formerly the Oak Ridge Gaseous Diffusion Plant) monitors designated areas of the plant for nuclear criticality. If a radiation-generating event were to occur, the system would provide both audible and visual alarms to initiate the evacuation of personnel from the danger area and simultaneously notify the plant emergency director's office that gamma radiation had been detected and indicate which instrument locations were involved in detection of the incident. Although the K-25 Site is no longer actively involved in enriching uranium, nuclear materials are still handled or stored in certain areas of the plant, and the RAS helps to ensure the continued safety of personnel in these areas.

The RAS, originally designed and installed in the early 1960s, employed dose-integrating, gamma-neutron-detector instruments arranged in clusters of three. The three instruments per cluster provided protection against false alarms by requiring two of the three instruments to detect radiation before an alarm was activated and also improved system reliability by overcoming instrument failures with redundant detection. In 1979, the publication of American Nuclear Standards Institute (ANSI)/American Nuclear Society (ANS) 8.3-1979 started the process that eventually resulted in a significant sensitivity upgrade in the RAS with the installation of new instrument clusters in 1985. Prior to the upgrade, the old clusters provided single coverage for all monitored areas, employing about 70 clusters with a stated coverage range of 68.6 m (225 ft). Since the old instruments were of the dose-integrating type, they could not meet the 0.5-s response requirement of the ANSI standard, needing as much as 60 s of integration time to alarm for a "minimum accident of concern" located 68.6 m away.

During the procurement of the new clusters in 1984, the U.S. Department of Energy requested that a single-failure analysis be conducted on the entire RAS. Technology for Energy Corporation (TEC) of Knoxville was contracted to perform the system analysis, while plant instrument development personnel were responsible for the internal analysis of the new clusters. The final TEC report (Stutzke and Dougherty 1984) described "only three potential failures (test/maintenance errors, short to ground in the local horn actuate solenoid, and the individual cluster reset switch) which could fail the system." At the same time, development personnel determined the existence of failure modes in the new cluster output circuitry that could interfere with its alarm signals. Based purely on avoidance of any further delay or economic impact on the upgrade, the decision was made to overcome the possible hardware failure modes by changing the alarm threshold of the new clusters from 40 mR/h [K-33 minimum accident scenario with heavy attenuation (Westfall and Knight 1984)] to 10 mR/h. This change extended the coverage range of the new clusters from 68.6 m to 121.9 m (400 ft) to provide overlapping coverage (H. R. Dyer and H. C. Jordan, letter dated March 23, 1984, to H. C. Webber, "Review of the ORGDP Alarm Coverage for: The Single Failure Analysis Study," Union Carbide Corporation, Oak Ridge Gaseous Diffusion Plant, Oak Ridge, Tenn.).

The new clusters were custom built for the K-25 system by Nuclear Research Corporation (NRC) of Warrington, Pennsylvania. They are configured much like the old units in that they still use three independent gamma-detector instruments, which are now rate sensitive and normally require two instrument alarms to generate a cluster alarm.

Each new cluster, however, is much more reliable because each monitors the operating status of its instruments and can generate a radiation alarm even if two of its detector instruments fail.

2. DOUBLE COVERAGE

Since the implementation of safety system configuration controls on the RAS on October 1, 1990, a critical situation exists in the availability of clusters for full double-coverage monitoring and for maintenance activities on the system. After the shutdown of the process buildings in 1985, RAS coverage in many areas of the K-25 Site was removed, leaving a surplus of instrument clusters. Soon thereafter, 32 clusters were shipped to the Paducah Gaseous Diffusion Plant to replace old clusters in the RAS there, leaving 51 units for use at K-25. Since that time, the monitoring philosophy at K-25 has become more stringent and has required reinstallation of clusters in many areas. With 50 clusters currently in use in the RAS, only one spare cluster is available for shop use and backup. To provide full double coverage for all designated areas, ~10 additional clusters are needed to fulfill current system requirements and provide Instrument Maintenance with adequate spares. The manufacturer of the new clusters, NRC, has been contacted about the purchase of additional units, and their estimated cost is ~$20,000 per cluster for a minimum order of 20 units and 6–9 month delivery. This estimate is almost three times the unit price paid in 1985.

3. SINGLE-FAILURE-PROOF CRITERIA

In the event of a radiation incident, the purpose of an RAS is to provide immediate detection and annunciation of the incident. The single-failure criteria for the K-25 Site RAS are interpreted to mean that no single failure in any part of the system shall be able to prevent the evacuation alarm annunciation in an affected area. For single coverage, the failure of an instrument cluster to detect and signal the occurrence of a radiation incident within its radius of coverage would then represent an unacceptable failure. The criteria do not consider that most criticalities postulated for the K-25 Site would result in alarms from many clusters, even with nonredundant coverage. For so-called single coverage by the RAS, the alarm must not fail to sound even if only one cluster can detect the incident.

4. SYSTEM CONSIDERATIONS

The single-failure criteria certainly do not dictate that every component in the RAS should be redundant, but it does require sufficient redundancy to guarantee an adequate system response to a radiation event. In practical terms, component failures can occur in a large distributed system such as the K-25 RAS, but their frequency is reduced with regularly scheduled system maintenance and testing, and their impact is minimized with status monitoring and strategic redundancy.

The K-25 system employs the extensive use of status signals from each cluster and building evacuation control cabinet; these status signals are displayed on the system map board in the K-1650 Central Control Facility (CCF). Most problems that could occur within a building or in a telemetry cable would be indicated immediately at CCF and quickly repaired. Since each building monitored by the system contains what amounts to a stand-alone alarm system, it has been determined that problems in a telemetry cable back to CCF, including complete severance of the cable, would not prevent an alarm in any buildings where detection occurs. The failure would, in addition, be indicated on the map board at CCF as a fault requiring immediate maintenance attention.

Severance of the cable between a cluster and its associated building evacuation control cabinet would prevent the actuation of a system alarm from that cluster, but it would not disable the cluster's local air/nitrogen horn. This type of failure is very unlikely to occur since these cables are enclosed in conduit. Such a problem would, however, be indicated on the map board at CCF should it occur. In addition, two alarm circuits, one of which is a normally open relay circuit, are carried in the cable from each cluster so that a short in a cluster cable would be more likely to cause an alarm than to prevent one.

Hardware redundancy in the K-25 system provides added protection that the system will not fail to respond in an emergency situation. Three instruments in each cluster provide continuous radiation level monitoring, and a cluster can alarm with one or even two instrument failures. Redundant alarm paths now in the cluster's redesigned output logic guarantee that its two output alarm relays will actuate to pass two alarm signals into the system. Because these signals follow separate alarm paths in the system, a failure in either path (cluster or system) would not prevent annunciation of the alarm condition.

Operating procedures currently require that system maintenance must be performed with that portion of the system in TEST mode, selected via one of the TEST/TROUBLE switches on the map board at CCF, to prevent false alarms. This mode disables the selected building evacuation control cabinet, building horns and lights, and slaved alarms to other buildings. Redundant cluster coverage does not provide an improvement in system coverage during these times, because several clusters are frequently connected to a common evacuation control cabinet. In this temporary mode of operation, however, the local air/nitrogen horns of any clusters detecting radiation would still provide immediate warning for personnel in the area, and the map board at CCF would also notify the plant shift superintendent (PSS) that radiation had been detected. If this situation were to occur, the PSS would then manually activate the building horns and lights in the affected area. The use of TEST mode, therefore, does not prevent the timely evacuation of personnel, and redundant cluster coverage does not provide additional protection.

5. CLUSTER MODIFICATIONS

The 1984 TEC analysis of the K-25 system determined that the system was not totally fail-safe. Three possible failure scenarios could be found that could interfere with the annunciation of an alarm. A recent reevaluation of the TEC analysis showed that two of the three failure scenarios were hardware related and that their effect depended on the configuration of the output logic circuitry in the cluster. An in-house redesign of the cluster output logic board has therefore been implemented to circumvent the identified system failures and to make the clusters themselves single-failure proof. The third TEC-identified failure mode, involving test/maintenance errors, could not be overcome with system hardware but is being addressed under system configuration control of the system through improved training.

The cluster modification involved the redesign and replacement of the circuit board in the cluster's output logic module. This board contains the logic circuitry, which receives the alarm and fault signals from the cluster's three detector modules and decides when alarm or fault signals should be sent to the system. The schematic diagram (Fig. 1) shows the cluster output logic circuitry as it was originally built by NRC. Analysis of the alarm path through the logic showed that a failure in any one of several gates or components on the board could totally inhibit a valid alarm condition. These failures included U1C, U3C, U3D, U4C, U6D, U7C, and Q2, so the redesigned board had to specifically provide dual signal paths in these areas. Although it had no impact on the final outcome of the modifications, one of the two hardware failures identified by the TEC study (a short to ground on the individual cluster reset switch) did not represent a true alarm failure scenario. This problem would result in actuation of the cluster remote reset relay, K1, which would momentarily reset the cluster logic through capacitor C8, but it would not inhibit a subsequent alarm.

The new cluster output logic design (Fig. 2) provides redundant alarm paths through the board and corrects several other potential problems in the original design. This design has been thoroughly reviewed and tested, and makes the cluster single-failure proof because no single undetectable failure on the board or in the cluster can totally inhibit both alarm output signals to the system. On the other hand, failure modes that could result in a false alarm are allowed to exist.

The new board can actually tolerate multiple logic-gate failures because the logic chips on the board have been arranged such that complete failure or removal of any integrated logic circuit will not inhibit an alarm. The board is also protected against the TEC-identified hardware failure mode, a short in the local horn-actuated solenoid valve. This failure not only could have resulted in permanent damage to the logic board but also could have totally inhibited all three alarm outputs. Protection against this failure is now provided by fuse F2 in the output line to the solenoid. Only one possibility for a disabling failure, the loss of the 5-V power to the board logic resulting from failure of the voltage regulator (U10) has been allowed to remain. This failure mode is considered to be acceptable because it would be indicated immediately as a cluster fault on the map board at CCF.

The new logic board (Fig. 3) was designed for installation in the cluster logic module as a direct replacement of the original board. The modification is now installed in every K-25 cluster.

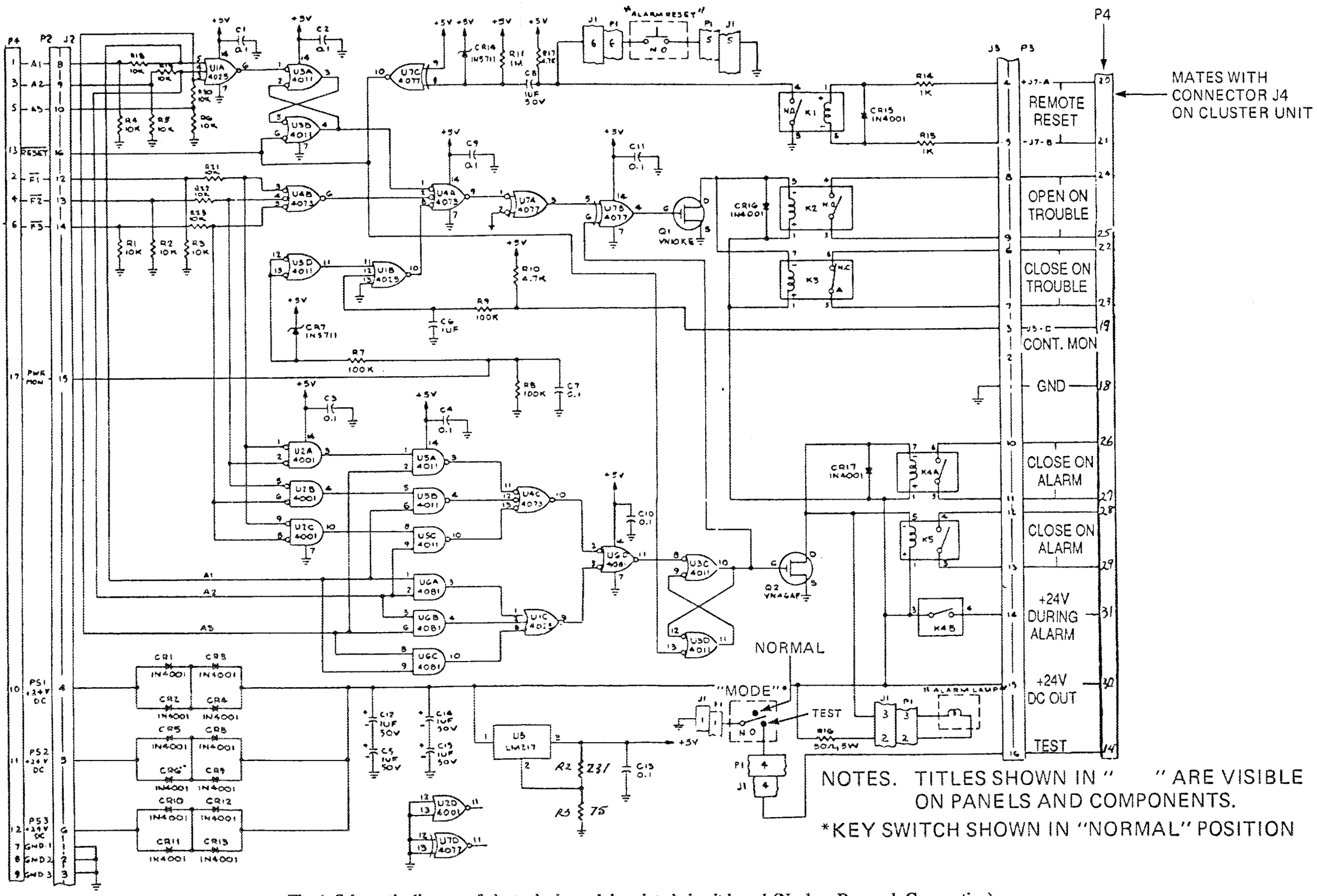

Fig. 1. Schematic diagram of cluster logic module printed circuit board (Nuclear Research Corporation).

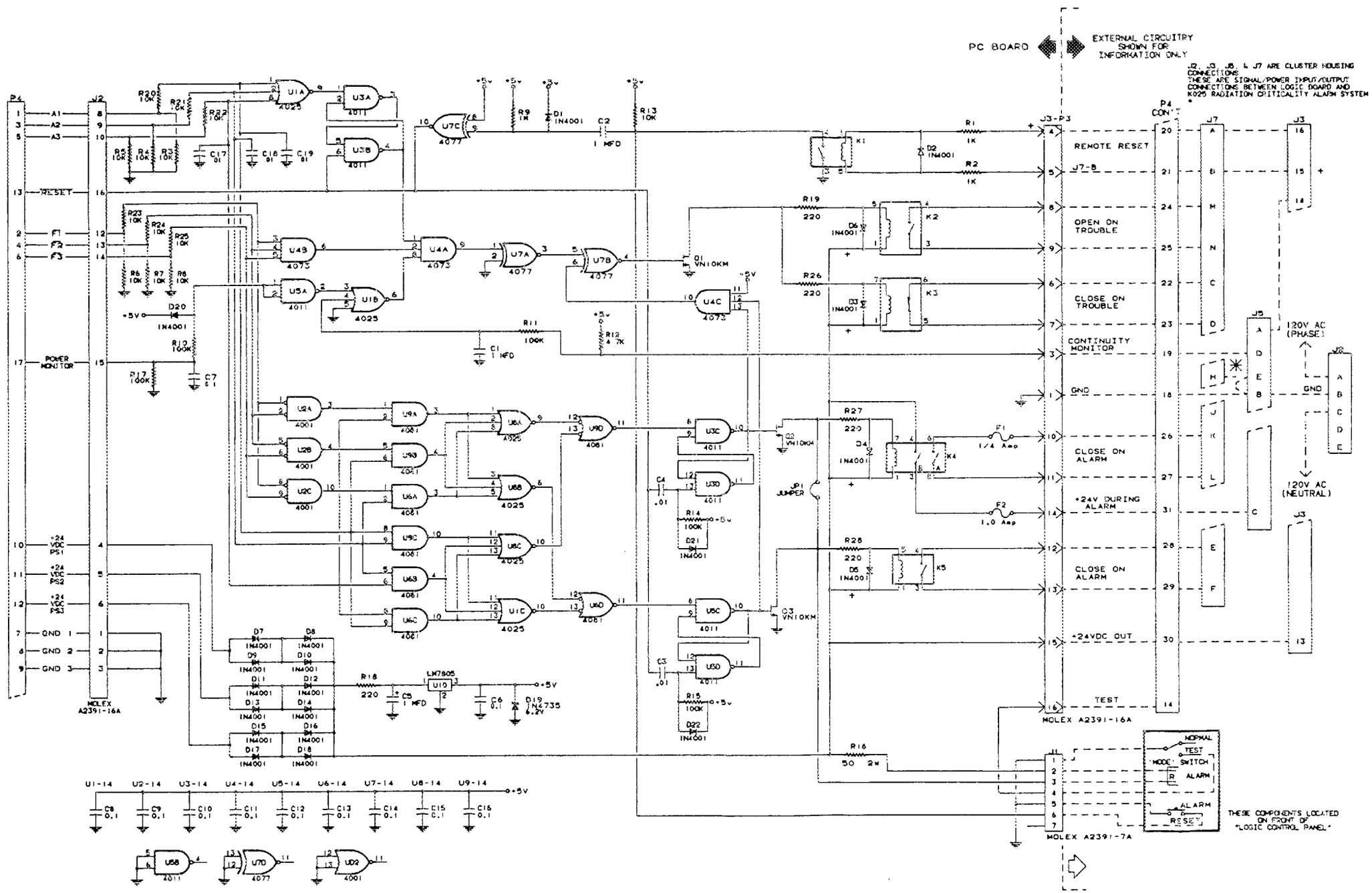

Fig. 2. Schematic diagram of cluster logic module printed circuit board (new).

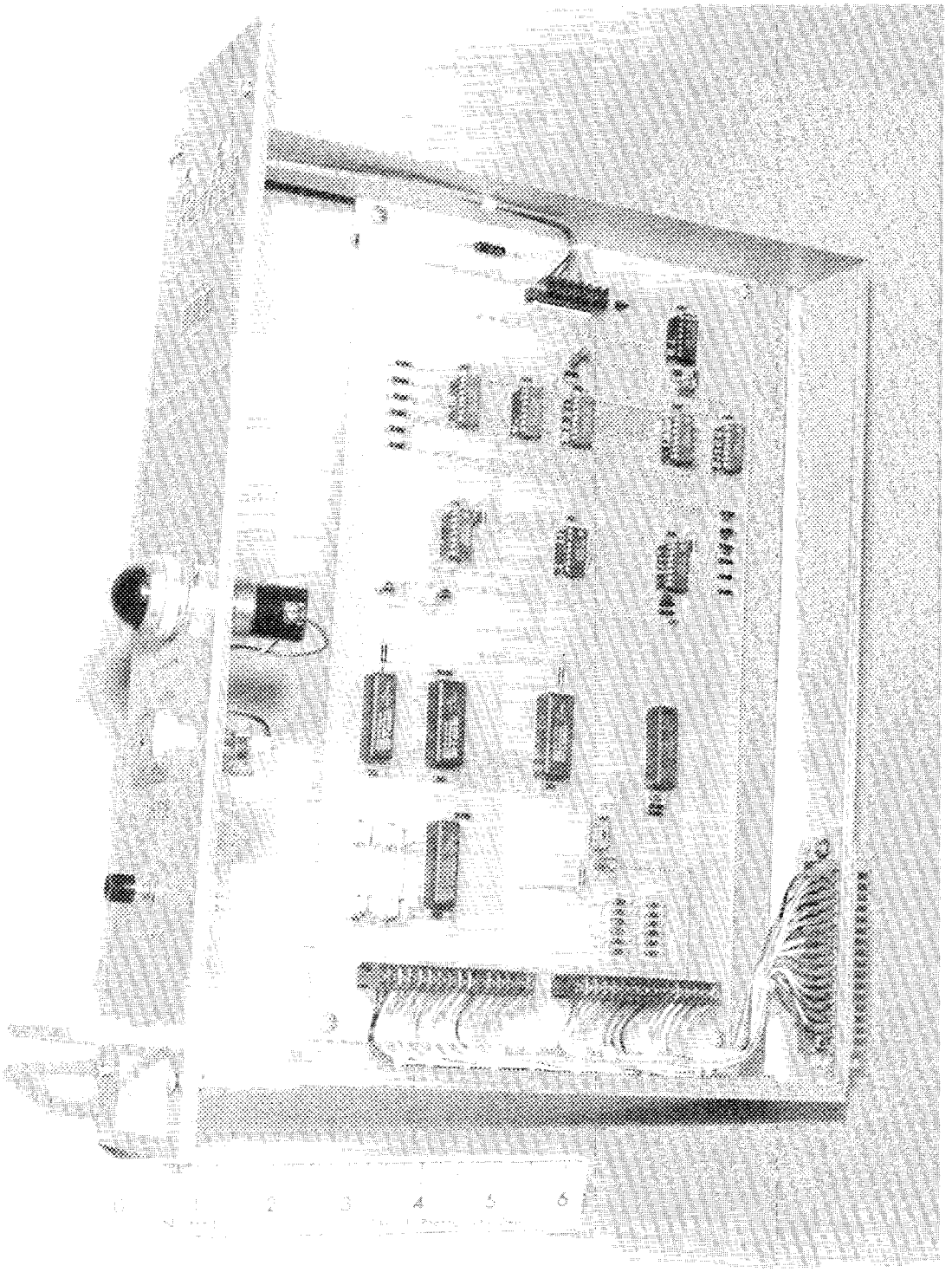

Fig. 3. Cluster logic module assembly.

6. FINAL COMMENTS

Because the clusters are now considered to be single-failure proof and redundant in themselves, the removal of redundant cluster coverage would not result in a reduction in the degree of personnel protection currently provided. The Criticality Safety Department at K-25 has analyzed the RAS single-coverage needs and found that 18 clusters currently providing redundant cluster coverage could be removed from service (J. C. Ingram, memorandum dated May 11, 1990, to J. D. Bolling, "Single Failure Modifications to the K-25 Radiation Alarm System," Martin Marietta Energy Systems, Inc., K-25 Site, Oak Ridge, Tenn.). Removal of these clusters would, in fact, improve the system by reducing its complexity and maintenance requirements. The return to single-coverage operation would also eliminate the need to acquire additional clusters at a cost of ~$400,000 and would result in a estimated yearly savings of $20,000 to $40,000 in system maintenance costs.

If single-cluster coverage operation is implemented for the RAS, the only time an area could be left with no detection or alarm coverage would be during maintenance activities when a cluster must be disconnected briefly from both the system and its local air/nitrogen horn. During these activities, maintenance procedures would be revised to require the use of a portable cluster and evacuation horn unit. This unit has been designed and fabricated, but a cluster is not yet available for installation in the final assembly.

REFERENCES

Sturzke, M. A., and E. M. Dougherty 1984. *Single Failure Analysis of the ORGDP Radiation Alarm System*, Technology for Energy Corporation, Knoxville, Tenn.

Westfall, R. M., and J. R. Knight 1984. *Radiation Levels in a Gaseous Diffusion Plant Assuming a Low-Enriched Criticality Event Corresponding to the ANSI-Standard Minimum Accident of Concern*, K/CSD/TM-55, Union Carbide Corporation, Oak Ridge National Laboratory, Oak Ridge, Tenn.

INTERNAL DISTRIBUTION

1. J. W. Amburgey, Jr.
2. J. E. Bluford
3. J. D. Bolling
4. J. T. Bradbury, III
5. H. R. Brashear
6–10. K. N. Castleberry
11. B. G. Eads
12. D. N. Fry
13. G. L. Grametbauer
14. J. E. Huffer
15. J. C. Ingram, III
16. D. W. McDonald
17. S. J. Mead
18. D. R. Miller
19. C. H. Nowlin
20. L. C. Oakes
21. L. D. Owens
22. S. S. Paulus
23. C. H. Peterson
24. E. W. Pritchard
25. C. P. Sampson
26. R. E. Uhrig
27. R. M. Westfall
28. H. D. Whitehead, Jr.
29. A. Zucker
30. J. B. Ball, Advisor
31. P. F. McCrea, Advisor
32. C. E. Sanders
33. T. B. Sheridan, Advisor
34–35. Central Research Library
36. Y-12 Technical Reference Section
37–38. Laboratory Records
39. Laboratory Records-RC
40. ORNL Patent Section
41. I&C Division Publications Office

EXTERNAL DISTRIBUTION

42. Office of Assistant Manager for Energy Research and Development, DOE-ORO, P.O. Box 2001, Oak Ridge, TN 37831-8600.

43–52. Office of Scientific and Technical Information, U.S. Department of Energy, P.O. Box 62, Oak Ridge, TN 37831.