UNCLASSIFIED

CENTRAL RESEARCH LIBRARY
DOCUMENT COLLECTION

MARTIN MARIETTA ENERGY SYSTEMS LIBRARIES
3 4456 0350135 1

ORNL-2090
Physics

cy. 4

A PHILOSOPHY OF CONTROL-SYSTEM DESIGN

E. P. Epler

CENTRAL RESEARCH LIBRARY
DOCUMENT COLLECTION

LIBRARY LOAN COPY

DO NOT TRANSFER TO ANOTHER PERSON

If you wish someone else to see this document, send in name with document and the library will arrange a loan.

OAK RIDGE NATIONAL LABORATORY
OPERATED BY
UNION CARBIDE NUCLEAR COMPANY
A Division of Union Carbide and Carbon Corporation
UCC
POST OFFICE BOX P · OAK RIDGE, TENNESSEE

UNCLASSIFIED

Printed in USA. Price 15 cents. Available from the

Office of Technical Services
U. S. Department of Commerce
Washington 25, D. C.

LEGAL NOTICE

This report was prepared as an account of Government sponsored work. Neither the United States, nor the Commission, nor any person acting on behalf of the Commission:

A. Makes any warranty or representation, express or implied, with respect to the accuracy, completeness, or usefulness of the information contained in this report, or that the use of any information, apparatus, method, or process disclosed in this report may not infringe privately owned rights; or

B. Assumes any liabilities with respect to the use of, or for damages resulting from the use of any information, apparatus, method, or process disclosed in this report.

As used in the above, "person acting on behalf of the Commission" includes any employee or contractor of the Commission to the extent that such employee or contractor prepares, handles or distributes, or provides access to, any information pursuant to his employment or contract with the Commission.

UNCLASSIFIED

ORNL-2090

Contract No. W-7405-eng-26

INSTRUMENTATION AND CONTROLS DIVISION

A PHILOSOPHY OF CONTROL-SYSTEM DESIGN

E. P. Epler

DATE ISSUED

JUL 12 1956

OAK RIDGE NATIONAL LABORATORY
Operated by
UNION CARBIDE NUCLEAR COMPANY
A Division of Union Carbide and Carbon Corporation
Post Office Box P
Oak Ridge, Tennessee

MARTIN MARIETTA ENERGY SYSTEMS LIBRARIES

UNCLASSIFIED

3 4456 0350135 1

ORNL-2090
Physics
TID-4500 (11th ed.)

INTERNAL DISTRIBUTION

1. C. E. Center
2. Biology Library
3. Health Physics Library
4-5. Central Research Library
6. Reactor Experimental Engineering Library
7-26. Laboratory Records Department
27. Laboratory Records, ORNL R.C.
28. A. M. Weinberg
29. L. B. Emlet (K-25)
30. J. P. Murray (Y-12)
31. J. A. Swartout
32. E. H. Taylor
33. E. D. Shipley
34. C. S. Harrill
35. M. L. Nelson
36. C. P. Keim
37. J. H. Frye, Jr.
38. R. S. Livingston
39. C. J. Borkowski
40. W. H. Jordan
41. S. C. Lind
42. F. L. Culler
43. A. H. Snell
44. A. Hollaender
45. M. T. Kelley
46. G. H. Clewett
47. K. Z. Morgan
48. T. A. Lincoln
49. A. S. Householder
50. C. E. Winters
51. D. W. Cardwell
52. J. A. Lane
53. E. M. King
54. W. J. Ladniak
55. D. D. Cowen
56. M. J. Skinner
57. S. J. Cromer
58. R. R. Dickison
59. S. H. Hanauer
60. R. A. Charpie
61. T. E. Cole
62. C. S. Walker
63. J. A. Cox
64. F. C. Maienschein
65. C. E. Clifford
66. L. B. Holland
67. L. C. Oakes
68. P. M. Reyling
69-92. E. P. Epler
93. ORNL – Y-12 Technical Library Document Reference Section

EXTERNAL DISTRIBUTION

94. R. F. Bacher, California Institute of Technology
95. Division of Research and Development, AEC, ORO
96-798. Given distribution as shown in TID-4500 under Physics category (300 copies – OTS)

DISTRIBUTION PAGE TO BE REMOVED IF REPORT IS GIVEN PUBLIC DISTRIUBITON

A PHILOSOPHY OF CONTROL-SYSTEM DESIGN

During the past decade a number of reactors of the heterogeneous light-water-moderated type have been designed and constructed at ORNL. These have ranged from the simple Swimming Pool Reactor to the larger and more complex MTR and ORR, with several intermediate types, all having many characteristics in common. The control systems for several of these reactors are now being modernized, so that it is an appropriate time to review past experience in order that the more desirable features may be incorporated in current designs.

Without exception each installation has required increased reactivity for operation at higher fluxes. Control rods and safety instruments have been added to provide adequate safety. Changes in operating practice have placed unanticipated demands on control systems. Early reactor designs were influenced by assurances of experimentalists that operation would be closely supervised by the head of the facility; invariably the responsible individual has turned his attention to other matters, leaving reactor operation to others. On some occasions the operating organization has been faced with the necessity of turning reactor operations over to groups only loosely associated with the Laboratory. To effect economy in operation, the LITR has been remotely operated from the control room of the Graphite Reactor on an experimental basis for almost a year. Work is under way leading to the remote operation of both the Graphite Reactor and the LITR by means of controls located in the ORR control room. Experience at the Bulk Shielding Facility (BSF) has made apparent the need for devices appropriate for unattended operation. It has been found advantageous to conduct preliminary operation of a new shielding reactor at the BSF, with final operation to be performed at the Tower Shielding Facility (TSF); the controls systems at both the BSF and TSF are required to be compatible with the new reactor.

As a result of changing demands, reactors built with emphasis on economy and limited reactivity, having served their initial purpose, have required almost complete rebuilding. Modern components incorporating all the desirable features are replacing the original equipment with no increase in cost.

These experiences have pointed up early mistakes and have shown the need for generalized control systems, incorporating methods of proven worth, which may be constructed quickly with standardized components and which are capable of meeting any reasonable performance demand so far encountered. As a step in this direction, modular assemblies of rod and chamber drives are now being used, as well as modular operating and relay subpanels associated with these drives. Benefits expected are: ease of expansion, reduced cost, and simplified installation and maintenance.

The Borax experiments have shown that, for the Swimming Pool type of reactor, it is almost impossible to experience a destructive accident through a short-period excursion if the excess reactivity can be rigidly limited. This development has necessitated a reappraisal of objectives in regard to safety-system performance. By being willing to

accept permanently a reactivity limitation, a simplification of safety systems might be in order. If, on the other hand, it is believed that increased loadings, shorter neutron lifetimes, and reduced heat transfer are ultimately inevitable, then a much higher degree of performance will be required of the safety system. Since all the experience at ORNL to date has been in the direction of increased demands on safety, the necessity for improved safety performance can be foreseen.

Small reactors with 24-in. rods having a total worth of from 8 to 10% $\Delta K/K$, together with fast safety systems, are capable of inserting significant amounts of ΔK during a short-period excursion. Safety systems now in use at ORNL incorporate magnets with release times of less than 5 msec, with an over-all delay time of the safety system of less than 10 msec. With rod accelerations of 1 g, in a typical case, an excursion with a period of 30 msec should be limited to a rise of ten times normal operating level by action of the level safeties alone. The addition of a derivative device capable of actuating the safety system at a point at least two orders of magnitude below normal operating level should be expected to limit a 10-msec-period excursion to a maximum rise of ten times normal level. Since the startup accident should generate a period no shorter than 100 msec, this is far better than the minimum performances required to contain a startup accident.

At ORNL it has been the general practice to provide only 1 g rod acceleration; however, the TSF has experienced two years of completely satisfactory operation employing 3 g's with direct-lift magnets. This has encouraged the belief that, with slight modification, equal operational reliability should be expected with accelerations up to 5 g's, which would limit, in the example above, a period of 15 msec by action of level safeties and a period of 7 msec by action of the derivative device.

Some consideration has been given to the application of explosives for fast shutdown. There would be a reluctance to actuating such a device by means of a derivative; therefore its operation would be required to begin at some point above the normal safety setting. To perform equally with a derivative-actuated release, accelerations of from 25 to 50 g's would be required. However, it is believed that, until existing methods have been more fully exploited, there is little incentive to resort to explosives.

Although the safety system may be capable of limiting the improbable short-period accident with somewhat less than absolute reliability, the primary role of the safety system must be to contain the inevitable startup accident with absolute reliability. To this end, some principles and practices have been established and rigidly followed:

1. Two independent safety systems are required to be in operation at all times. The inoperability of one of two systems demands immediate shutdown of the reactor. To obtain freedom from mandatory shutdown on a symptom of trouble in one safety system, three independent systems are required.

2. Complete monitoring of the safety system is necessary so that any conceivable fault will be unnunciated.

3. The setting of the trip level of the safeties is not altered for any reason other than a permanent change in the reactor operating level. Any advantages which might accrue from reduced setting at startup are also obtainable from the period safety and from other devices.

4. The use of coincidence safeties, popularly known as "two out of three," is not practiced. It has been true generally that accidental shutdowns of unknown cause have been classified in the operating records as safety troubles. Most bona fide safety troubles occur as faults in the incoming power supply, in the wiring external to the safety electronics, and in the condition of the magnet pole faces. None of these will be minimized by placing the safety devices in coincidence; therefore it is believed that the principal effect will be a reduction in safety.

5. The use of safety instruments for any function other than safety is forbidden.

Mechanical rod drives have often violated safe practice and, in addition, have offended in the omission of vital parts necessary for a smoothly operable control system.

Rods suspended by tapes or wires are subject to upward movement not governed by the control system. In the worst case they may be expelled from the reactor in a minor accident, thus creating a major accident. A variation is the rotary clutch which disconnects the rod from its motor drive on action of the safety release; this permits the rod to move upward or downward dependeng on the net forces. An additional fault lies in the inability of the motor to force the rod into the reactor during an emergency.

The most common cause of false release in direct-lift magnets is the accumulation of trash and magnetic particles in the pole faces. This has been minimized by the provision of automatic follow-up such that, after release of the rod, the magnet current is blocked off and the motors are caused to drive the magnet down. Motion is stopped, and magnet current is reapplied after the pole faces are mated at the end of the stroke. This and other advantages are lost when the drive mechanism is deficient in limit switches. The following is the standard complement, of which the omission of any one will result in an unacceptable drive:

1. upper limit of motor travel,
2. lower limit of motor travel,
3. rod seated on bottom,
4. rod in contact with magnet.

In establishing the maximum rate of reactivity change at startup, it is assumed that all rods will be withdrawn together. No dependence is placed on sequencing devices or interlocks, which on failure will grossly increase the withdrawal rate. For the same reason the withdrawal and insertion speeds of the drive are identical so that no conceivable accident in direction can increase the withdrawal rate. Further advantages in

withdrawal of all rods simultaneously accrue in that the rods will be in a position of maximum sensitivity during startup.

It is assumed that a failure of the control system will ultimately cause a startup accident in spite of good design practice. Three-phase motors can be reversed in direction of rotation through a phase reversal outside the premises. Wiring faults will cause the motors to run in spite of control action. These weaknesses can be minimized or eliminated but others will crop up. It is believed that undue preoccupation with this problem will result in immobilization of the control system. The existence of a fully monitored, fast, and reliable safety system which reduces the startup accident to trivial proportions should be exploited to permit the control system to be designed for the maximum convenience consistent with good practice.

The instrument start feature which is being incorporated in most of the ORNL reactors now being designed is a logical consequence of practices adopted in earlier reactors. This feature is not a gadget which has been added but is more aptly described as a full complement of control devices which, when all conditional requirements have been met, permit the operator to select the automatic button for rod withdrawal, which will remain latched until the servo has assumed control at the selected operating level. Most of these devices and methods have been in use for a number of years, and it has been necessary only to add a few refinements.

Contacts in the log n period recorder have been used to stop rod withdrawal on the occurrence of a suitable startup period. Similar contacts on a count-rate period recorder cover the lower ranges, giving continuous period supervision from source-range to full-power operation. Other contacts on the same recorders initiate rod reversal on the occurrence of unsuitably short periods. It should be noted that this period protection exists whether the reactor is being started manually or under instrument supervision and that any number of available period channels may be added for increased reliability.

Before withdrawing shim rods, the practice has been to turn on the servo, which will withdraw the regulating rod to its upper limit. When the flux has reached the desired operating level at the conclusion of startup, the servo will insert the regulating rod to maintain that level without further attention from the operator. Duplicate instructions as to the desired operating level are transmitted to the log n recorder, which will cause shim-rod insertion if for any reason the flux exceeds the desired operating level. Again, these protection measures exist whether the reactor is being started manually or under instrument supervision.

The principal remaining ingredients of the instrument start feature are monitoring interlocks which ensure that instruments are in operating condition and are properly ranged. When these and some other lesser refinements are present in a control system, the rod withdrawal button may be latched in withdraw position, to be unlatched after desired flux level is reached, or upon malfunction of the control system. It is submitted

that the instrument start feature is not an added device but that it is evidence that a complete control system exists.

Larger research reactors must accommodate simultaneously a number of experiments with varying degrees of coupling with the reactor. Many of these experiments will require more extensive control systems than the reactor itself and may sometimes suffer from hasty construction and improvisations. If the reactor is scrammed on occurrence of all minor troubles, operations will frequently be interrupted, and as a result there will be a reluctance to apply as many protective features as may be desired. It is unfortunately true that the reduction of reactor power will probably not alleviate the difficulty at the experiment and in some instances will create an emergency in another experiment. However, a reduction of reactor power is considered to be the prudent course until the trouble can be cleared and appraised.

To meet these requirements, a system has been devised which has been in use for several years with fair success and which is being incorporated in current work.

Reactor power is normally reduced through setback, which is a continuous reduction of the servo set point. A logarithmic potentiometer which is motor driven will reduce the power level so long as the trouble persists or until the level is reduced to 1% of normal. Momentary faults will then cause the minimum amount of disturbance to operations.

The scram is reserved for cases in which the reactor power must be reduced as rapidly as possible. It is also used as a backup for the setback so that if a requested setback is not obtained a scram will result.

For each type of corrective action, two channels of communication are provided between the reactor and the experiment. Reactor shutdown will be initiated for either an open-circuit or a closed-circuit fault in the interconnecting cable.

Although this system is non-fail-safe, there have been no failures to obtain corrective action when needed; however, the occurrence of unnecessary shutdowns is still greater than desirable.

After a safety system of unquestioned reliability has been provided and a control system has been devised which will automatically start the reactor, what is the role of the operator? First, as an example, postulate that the reactor is to be started and that calculations predict that criticality is to be attained when the rods have been withdrawn to a predetermined point. When that point has been reached, the rods are still being withdrawn, and it is obvious that the reactor is not critical although the instruments seem to be performing normally. Should the operator permit the startup to continue? If he is capable of acting only on information derived from instruments, he may be inclined to withdraw the rods further. If, on the other hand, he instantly recognizes that a dangerous situation exists, he will halt the operation and investigate. The true situation in this hypothetical case is that the control rod has become jammed in the partial fuel element from which it is being withdrawn. This is not unreasonable, because trash can become

lodged between the rod and its fuel element. The locking pin which ordinarily holds the fuel element in place has been omitted or has become weakened, so that the fuel element as well as the rod is being withdrawn from the approximate center of the reactor. At any moment the fuel element will fall back, and the reactivity will be increased by 2 or 3% $\Delta K/K$ in a time as short as $\frac{1}{4}$ sec, which will almost certainly result in the destruction of the reactor.

In this instance no instrument has failed. No instrument exists which will infallibly compute the reactivity at all times and will stop the process when the predicted rod position has been reached. If the accident is consummated, it must be charged solely to human failure.

It must be concluded that as instruments and controls become more reliable there is less justification for the existence of an operator who is capable only of receiving and acting on information derived from instruments. More boldness in operating procedures is in order where instrument failures can cause only minor accidents; the maximum of operator ability and alertness will be required to avert the more serious accidents.

BIBLIOGRAPHY

Jordan, W. H., "A Philosophy of Reactor Control," *Reactor Sci. Technol.* **2**(2), 81 (September 1953).