AN EVALUATION OF THE
EBR-II FUEL-HANDLING COMPLETE CIRCUIT

by

R. O. Haroldsen and R. N. Curran

EBR-II Project
Argonne National Laboratory
Argonne, Illinois - Idaho Falls, Idaho

March 1972

NOTICE

This report was prepared as an account of work sponsored by the United States Government. Neither the United States nor the United States Atomic Energy Commission, nor any of their employees, nor any of their contractors, subcontractors, or 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.

TABLE OF CONTENTS

	<u>Page</u>
ABSTRACT	4
I. INTRODUCTION	4
II. DESCRIPTION OF FHC CIRCUIT	5
III. HISTORY OF FHC CIRCUIT	8
IV. APPROACH	10
V. CONNECTOR MONITORS	11
A. Description	11
B. Evaluation	11
1. Possible Connector Malfunctioning	11
2. Consequence of Faults	12
a. Open Circuit	12
b. Short Circuit to Ground	12
c. Short Circuit Between Conductors or to Power . .	13
C. Recommendations	15
VI. REACTOR-COVER-LOCK MONITORS	15
A. Description	15
B. Evaluation	19
1. Safety Considerations	19
a. Probability of Malfunction	20
b. Consequences of Malfunction	20
C. Recommendations	23
VII. MISCELLANEOUS MONITORS IN THE FHC CIRCUIT	25
A. Description	25
B. Evaluation	27
C. Recommendations	28
VIII. CONCLUSION	28
REFERENCES	29

LIST OF FIGURES

<u>No.</u>	<u>Title</u>	<u>Page</u>
1	Fuel-handling Complete Circuit	6
2	Simplified Control Circuit for Primary-pump MG System	7
3	Trip Circuit for Primary Pumps	9
4	Fault-tree Analysis of Short Circuit in Rotating-plug Connectors	14
5	Cover-locking Mechanisms of the EBR-II Reactor Vessel	16
6	Tie-rod Center Shaft and Guide Tube of Cover-locking Mechanism of the EBR-II Reactor Vessel	17
7	Drive Assembly of Cover-locking Mechanism of the EBR-II Reactor Vessel	18
8	Pressure Differential Across Reactor-vessel Cover with Inadvertent Closure of Sodium Outlet of Vessel and Vertical Gap at Vessel Top Flange	21
9	Fault-tree Analysis of Malfunctioning of Cover Locks	24

AN EVALUATION OF THE EBR-II FUEL-HANDLING COMPLETE CIRCUIT

by

R. O. Haroldsen and R. N. Curran

ABSTRACT

The fuel-handling complete (FHC) circuit of EBR-II has been evaluated as part of a larger effort on upgrading the plant protective system. The FHC circuit monitors 36 separate parameters. The reactor and primary pumps are subject to shutdown from any of the parameters monitored. The primary purpose of the monitors is to ensure that fuel-handling operations are properly terminated before reactor operations are undertaken. Equivalent protection can be obtained by modifying the circuit to enforce proper procedure in terminating fuel-handling operations without spurious reactor and pump trips.

I. INTRODUCTION

The "Fuel-handling Complete Circuit" (FHC Circuit) operates in the reactor shutdown circuit to prevent operation of the reactor and the primary-system coolant pumps except when all prerequisite conditions of the FHC circuit are satisfied; i.e., its primary purpose is to assure that plant conditions imposed by fuel handling that are incompatible with reactor operations are returned to normal before reactor startup.

The present FHC circuit enforces these conditions during reactor operation. Trip signals from the FHC circuit are particularly significant because shutdown of the primary-system coolant pumps is imposed simultaneously with reactor shutdown. Spurious trips* of the FHC circuit have

* Spurious trips are here defined as trips that originate from a malfunction of the plant protective system rather than from an unsafe condition.

been few (only one from full power). This infrequency is remarkable, because there are 36 independent trip functions (including those for INCOT) in the FHC circuit. On the basis of probability, a higher incidence of spurious trips would be expected.

This study is part of a plan to upgrade the FHC circuit to meet, to the extent practical, the criteria of RDT Standard C16-1T.¹

II. DESCRIPTION OF FHC CIRCUIT

Figure 1 shows the FHC circuit schematically. The required conditions monitored by the circuit are:

Reactor cover must be down;

Three cover-holddown springs must be compressed;

Three cover locks must be in locked position;

The sequence-A (beginning steps of fuel handling) relay must be unlatched;

The sequence H- (terminating steps of fuel handling) relay must be unlatched;

Key switch KS2 must be off;

Eighteen 100-pin connectors must be connected in proper location;

Three rod-oscillator connectors must be connected;

Two instrumented-subassembly connectors must be connected;

Instrumented-subassembly must be down;

Instrumented-subassembly yoke must not be retracted; and

Instrumented-subassembly yoke must be engaged.

A trip signal from any of the 36 items not only scrams the reactor but also shuts down the two main primary-system pumps.

Figure 2 is a simplified control diagram of the primary-pump M-G system. The diagram shows that the operation of the primary pump is subject to shutdown not only by the FHC circuit but also by the low-pump-speed monitor and the plenum-pressure monitor at the reactor outlet. The reactor is in turn subject to scram by the pump monitor circuit, which is shown schematically in Fig. 3. Pump parameters in the shutdown circuit that are monitored are:

Fig. 1. Fuel-handling Complete Circuit

Generator breakers: open (2);
Pump motor: phase current (4);
Clutch: reference voltage (2);
Clutch cooling water: pressure (2);
Pump-motor winding: temperature (2); and
2400-V supply voltage breaker: open to either MG set (2).

The 2400-V bus-voltage monitor (not shown in Fig. 3) could also be included in the list because its primary function is to monitor the power available to the pump M-G sets. All the pump trip circuits serve an anticipatory function for coolant-flow failure; they are being considered for deletion from the reactor shutdown circuit (see Ref. 2). For documentation in support of the deletion, see Ref. 3.

III. HISTORY OF FHC CIRCUIT

The original FHC circuit included the reactor cover, fuel-handling sequence, and key switch monitors. The 23 connectors and three instrumented-subassembly monitors were added to the circuit after completion of the original reactor plant.

The FHC circuit was primarily intended as a permissive circuit for startup. Most of the other permissive circuits in the EBR-II PPS are bypassed once the prerequisite conditions of the shutdown circuit are satisfied. The FHC circuit, however, remains active through all phases of reactor operation.

Once the prerequisite conditions imposed by the FHC circuit are satisfied, there is a very limited possibility of these conditions reverting to unsafe conditions. No attempt was made by the original designers to evaluate the probability of such reversions. Instead, they accepted the possibility; and, on this assumption, the FHC circuit was designed to remain active throughout all stages of reactor operation.

The 100-pin cable-connector monitors were added to the FHC circuit in the early checkout period of the reactor. Monitors were incorporated as a convenient way to assure that the cables would be properly reconnected after fuel-handling operations before reactor operations were started. Some difficulties were experienced in properly reconnecting the connectors after fuel handling. Also, the connectors might be connected in the wrong order

Fig. 3. Trip Circuit for Primary Pumps

because most of them are mechanically identical. The cable-connector monitors verify proper connection by a continuity test. Different test pins are used for the test circuit on each connector so that all connectors must be mated in the correct order to satisfy the requirements of the circuit. The same circuit requires that all connectors be disconnected to satisfy the requirements for fuel handling.

A difficulty with the monitor system is that it has the undesirable potential of tripping the primary pumps as well as the reactor during full-power operation. If the monitors had been incorporated into a new circuit independent from the FHC circuit, the new circuit almost certainly would have been designed only as a permissive requirement for reactor startup, and tripping of the primary pumps would have had no part in the circuit.

The cable and position monitors associated with the oscillator rod and instrumented subassembly were added later to the FHC circuit by the same logic as had been used for the 100-pin connector monitors. With these additions the FHC circuit included 36 different tripping functions.

IV. APPROACH

Upgrading the FHC circuit has been approached by following the guidelines and philosophy of RDT Standard C16-1T (see Ref. 4). This approach is as follows:

A. An attempt is made to identify all of the credible faults that could occur for each of the 36 items monitored by the FHC circuit.

B. The consequence of each fault is evaluated and probability of each is estimated by following the guidelines of the RDT Standard.

C. The monitors of the FHC circuit are evaluated with the aid of fault-tree analysis for their need and adequacy to prevent unacceptable damage.

D. A proposal is formulated recommending the disposition of the FHC-circuit components while meeting as far as possible the criteria of the RDT Standard.

The Standard divides fault probability into three categories: (1) Anticipated Faults; (2) Unlikely Faults; and (3) Extremely Unlikely Faults. An Anticipated Fault is an off-normal condition that may be expected to

occur at least once during the lifetime of the plant. An Unlikely Fault is not expected to occur during the lifetime of the plant but, when integrated over many similar plant components, may be expected to occur at least once. An Extremely Unlikely Fault is an off-normal condition that is not expected to occur during the lifetime of the plant but nevertheless is identified as possible.

The Standard defines four levels of accident severity: (1) Operational Incident; (2) Minor Incident; (3) Major Incident; and (4) Design Basis Accident. In an Operational Incident, there is no significant loss of effective lifetime of plant components. In a Minor Incident, damage is limited to some specified loss of effective lifetime of replaceable plant components. In a Major Incident, damage requires replacement or repair of replaceable and semipermanent plant components. The Design Basis Accident is a hypothetical accident of extremely low probability in which the primary barrier is involved.

V. CONNECTOR MONITORS

A. Description

The eighteen 100-pin connectors are numbered 1-8 through 18-8. Connectors 1-8 serves control rod No. 1 exclusively; similarly, connectors 2-8 through 12-8 serve control rods 2-12 exclusively.

Connector 15-8 carries 480-V-motor-power and rod-position signals for control rods 1, 2, 9, 10, 11, and 12. It also has connections serving the cover lift and cover-lift-column glands. Connector 18-8 is similar to connector 15-8 except that it serves control rods 3, 4, 5, 6, 7, and 8. Connectors 13-8, 14-8, 16-8, and 17-8 serve the control-rod-lifting platform, the cover-lifting mechanisms, and the thermocouples in the support columns. The five remaining connectors serve the oscillator rod and the instrumented subassembly.

B. Evaluation

1. Possible Connector Malfunctioning

The possible connector malfunctions are: (1) open circuit, (2) short circuit to ground, (3) short circuit between conductors, and (4) short circuit to power.

The probability of each of the possible malfunctions cannot be accurately defined but can be estimated within the scope of the RDT Standard from operating experience.

Open circuits in the connectors are expected. They have occurred and probably will occur again within the life span of the reactor. Short circuits between conductor or to ground are less likely than open circuits and are considered unlikely. Short circuits to power are even less probable and are considered extremely unlikely.

All of the cable-connector faults discussed here are most likely to occur as a result of fuel-handling operations. System checkout after fuel handling greatly reduces the probability that reactor operations will be affected by faults in the cable connectors.

2. Consequence of Faults

a. Open Circuit

Open-circuit faults in any of the 20 connectors introduce passive malfunctions of the equipment served by the circuits affected. A malfunction would most likely result in failure of the equipment to respond to command. Loss of, or error in, data for temperature and position and single phasing of three-phase motors are also possible.

The control-rod drives are the most sensitive equipment served by circuits that pass through the monitored connectors. The open-circuit fault of a connector serving a control rod will cause the rod to either scram or stop. If the rod does not scram, it will remain responsive to a scram signal. For the special case of single phasing of the control-rod-drive motor, an extremely unlikely possibility exists that the motor may still have sufficient torque (although much reduced) to move the rod. The direction of the motor rotation is predictable in this case because the loading of the control rod is sufficient to assure that any motion will be downward.

b. Short Circuit to Ground

A short circuit to ground within the connectors may produce any of the situations described in the previous section. It may also

interrupt power on one or more branch power circuits. All of the mechanisms served by the connectors are designed to respond to power failure either in an as-is or fail-safe condition. Control-rod scram will occur if the latch power is interrupted. If the latch power is not interrupted, the rod will remain responsive to the shutdown circuit even if power to other rod functions is lost.

c. Short Circuit Between Conductors or to Power

A short circuit between conductors within the connectors can produce any of the situations described in the previous two sections. It may also inject unwanted signals and voltages on any of the conductors in the connectors. Some of the connectors have conductors that operate at 480 V, but these conductors are grouped and isolated within the connectors by a band of unused connector pins.

A short circuit to power is a special case of short circuits between conductors. It may damage system components, but more important are the possible effects it may have on control-rod response. If the control-rod-latch solenoid could become shorted to a 90-V dc power source, the rod could become unresponsive to a scram signal. This possibility does not exist, however, because there are no voltage sources, except the normal source, inside the connectors great enough to hold the latch solenoid closed. The greatest possible short-circuit voltage available in the connector, excluding the 90-V dc latch power, is 120-V ac, which is not enough to hold the latch circuit closed. Connectors having 480-V ac conductors are not used in conjunction with the latching circuits.

If the control-rod-drive motor becomes connected to the three-phase 480-V power because of a short circuit (coherent short circuit), the rod may begin to travel either up or down at its normal rate of speed--the most serious consequence that can occur from shorting within the connectors. Control of one rod could be lost, but the remainder of the PPS would remain unaffected by the event. The cable-connector monitors have no influence on the event and there is no relationship between the event and the need to secure the primary pumps. Figure 4 shows a fault-tree analysis of the event. The consequence of the event would be less severe than described in Section 7.2.1 of ANL/EBR-048⁵ for a two-rod-insertion fault.

Fig. 4. Fault-tree Analysis of Short Circuit in Rotating-plug Connectors

C. Recommendations

The cable-connector monitors perform a worthwhile function--to verify that, after fuel-handling operations, the cable connectors are not only re-connected but are also reconnected in the correct order. The desirable function of the cable-connector monitoring circuit is enforcing a prerequisite condition for reactor startup. This feature can be retained while all other functions are removed from the main shutdown and pump-trip circuits. Removing these functions, which does not conflict with the RDT Standard, is recommended.

VI. REACTOR-COVER-LOCK MONITORS

A. Description

Seven trip circuits are used to verify that the reactor cover is down and locked during reactor operation. Conditions required for reactor operation are: (1) reactor cover is down, as indicated by a limit switch located on one of the cover-lift lead screws; (2) each of three cover locks is in the locked position, as indicated by a position-limit switch on each of the cover-lock drive mechanisms; and (3) each of three cover-holddown springs is compressed to at least 25,000 lb, as indicated by a position-limit switch detecting the spring deflection on each of the cover-lock mechanisms. A trip signal from any of these seven circuits starts reactor scram and shuts down the primary pumps.

A complete description of the cover-lock mechanism is in Vol. II, Chapter 5, Section 5.3, of the EBR-II Systems Design Descriptions (SDD).⁶ Figs. 5, 6, and 7 from that source show the mechanism. The main consideration in designing the cover-lock mechanism was to ensure that the cover would remain firmly seated to the reactor-vessel flange during normal operation of the reactor. The measured operating pressure is between 6 and 7 psi, and a pressure monitor is set to trip at 7.5 ± 0.5 psi. A pressure of 8 psi acting on the approximately 6060-in.² area of the lower surface of the cover would produce a total lifting force of about 24 tons. The cover weighs slightly less than 14 tons. The spring clamping force of each of the three cover locks can be adjusted to a maximum of 40,000 lb; they were factory-adjusted for 32,000 lb. If the differential pressure exceeds 19 psi with this spring setting, the springs will further compress and the cover will begin to lift.⁶

Fig. 5. Cover-locking Mechanisms of the EBR-II Reactor Vessel

Fig. 6. Tie-rod Center Shaft and Guide Tube of Cover-locking Mechanism of the EBR-II Reactor Vessel

Fig. 7. Drive Assembly of Cover-locking Mechanism of the EBR-II Reactor Vessel

B. Evaluation

1. Safety Considerations

Safety considerations for the cover locks are related to the following

a. Failure of the reactor cover to lock in the down position after fuel handling, followed by the cover lifting or tilting when the primary pumps are energized.

b. Lifting of the reactor cover during reactor operations because of higher-than-normal operating pressure in the reactor-outlet plenum.

c. Malfunctioning of one or more cover locks during reactor operation.

d. Binding or movement of the control rods due to tilting and lifting of the cover.

The normal operating pressure in the reactor outlet plenum is high enough to lift the cover if the cover locks are not in place. The lifting force would be quickly reduced as the cover lifts and permits the sodium flow to bypass the heat exchanger. With no tilting, the maximum lift is less than 0.22 in. With tilting, the maximum lift is difficult to calculate. However, the angle of tilt at which binding of control rods begins to take place has been calculated. The nominal clearance of the control-rod shafts is 0.030 in., and the labyrinth seal is 12 in. long. According to the above data, interference would begin when the tilt exceeds 0.23 in. on the outside diameter of the reactor cover.

If the cover locks were left open, the cover would lift when the primary pumps are energized (existing interlock and alarm circuits are not considered here). With available information, we do not know whether the cover would tilt or, with tilting, if the control rods would bind. However, the reactor is always shut down when the pumps are energized. Therefore, control-rod movement due to binding and cover motion for this case will begin from the normal shutdown position and will be too small to cause a nuclear incident.

The cover can lift or tilt during operation only if the normal reactor-outlet plenum pressure is greatly exceeded or if the cover locks fail. The reactor cover is designed to withstand about 100 psi without struc-

tural damage. This pressure slightly exceeds the maximum output pressure of the primary pumps. According to the SDD, the reactor cover would lift 0.23 in. at this pressure, and the maximum internal pressure resulting from full blockage of the sodium outlet would be limited to 35 psi; at this time the cover will have lifted 0.22 in. Figure 8 shows the calculated cover lifting for varying conditions.

The weakest link in the cover-lock mechanism is the bayonet lock on the center tie-rod shaft, which would malfunction at about 41 psi. The pressure would then equalize at 35 psi. The cover-lift mechanism is designed so that it cannot apply any downward force on the reactor cover.

A computation indicates that two of the three cover locks would be enough to prevent lifting or tilting of the cover for all normal operating conditions. At an assumed holding force of 32,000 lb for each of two cover locks, the outlet differential plenum pressure would have to exceed 8.6 psi to cause the cover to lift.

a. Probability of Malfunction

Probabilities have been estimated for the various possible cover-lock malfunctions, with no interlock circuitry assumed. Improper locking of the cover due to operator error is unlikely; i.e., it is not expected to occur during the plant lifetime. Operating procedure requires locking the cover, and failure to do so is annunciated.

The cover can be lifted during reactor operation only if either the holddown mechanisms malfunction or substantial overpressure in the reactor outlet plenum occurs. The holddown mechanism is overdesigned by a factor of about 6. The overpressure necessary to lift the cover is about three times the normal operating pressure. Neither of these events is expected to occur during the plant lifetime; therefore lifting of the cover during reactor operation is extremely unlikely.

b. Consequences of Malfunction

Failure to lock the reactor cover down through operator error, with subsequent energizing of the primary pumps, does not constitute a nuclear hazard to the reactor. It does, however, present some limited

Fig. 8. Pressure Differential Across Reactor-vessel Cover with Inadvertent Closure of Sodium Outlet of Vessel and Vertical Gap at Vessel Top Flange

possibility for damage to such hardware as the cover lock, cover drive, and the shafts that penetrate the reactor cover. There is a limited possibility that core subassemblies would lift from pump pressure, but only if the hydraulic holddown of the subassemblies were somehow not fully effective and the reactor cover were significantly raised.

Lifting of the reactor cover during reactor operations due to operating pressure higher than normal is not a malfunction of the cover-lock mechanisms, but it has similar consequences. At least part, and perhaps all, of the primary-coolant flow will bypass the heat exchanger. Depending on reactor power, the bulk-sodium temperature will increase but at a rate that is clearly within the response capability of the plant protective system, exclusive of the reactor-cover monitors.

Lifting of the cover by failure of one or two cover locks during reactor operation is the most serious cover-lock malfunction, although extremely unlikely. Tilting of the cover is almost certain to occur, but no determination can be made about binding of the control-rod drives. Binding of the control-rod drives resulting from lifting of the reactor cover depends on whether, and how much, the cover tilts. If the cover lifting is due to malfunctioning of one or two of the three holddown mechanisms, the cover will probably tilt. Cover lifting due to overpressure in the outlet plenum may or may not cause tilting. Because neither tilting nor binding is predictable within the necessary limits, the worst-case assumption is made that there will be control-rod binding if the cover lifts. The probability of rod binding is therefore assumed to be the same as for cover lifting, i.e., extremely unlikely. However, because of lack of precise knowledge, the assumption is made for this analysis that cover tilting, rod binding, and rod lifting all occur. The maximum amount that the rods might lift, and the possible effects on reactivity and reactor power, have been investigated.

Lifting of a control rod is resisted by a force equal to the weight of the rod minus buoyancy (about 200 lb) plus the downward force applied by the air cylinders (375 lb). For this evaluation it is assumed that this force would be overcome when the nominal clearance of the cover-rod seals is used up by tilting of the cover. It was stated earlier that: this clearance will tolerate a cover tilt of 0.23 in. on the outside diameter of the reactor cover before binding will occur; and the maximum uniform lift of the cover for any applicable situation will not exceed 0.22 in. For this

evaluation it is assumed that one edge of the cover may lift twice this amount while the opposite side does not lift. With this assumption, the average rod may lift as much as 0.11 in. If the reactor is in operation most of the rods are assumed to be banked about to the 10-in. level, where a typical rod is worth about 9 Ih/in. Ten rods moving an average of 0.11 in. would then cause a reactivity change of about 10 Ih.

The effect of the reactivity change on reactor power can be estimated by multiplying the reactivity change by the appropriate value for PRD (Power Reactivity Decrement). The average PRD over the entire power range of the EBR-II is about 1.7 Ih/MWt , but at full power the value is considerably reduced from the average value. An approximate value of 1 Ih/MWt is obtained by taking the slope of a typical PRD curve at 62.5 MWt . This value leads to the conclusion that the ultimate steady-state power change that would result from a reactivity increase of 10 Ih at 62.5 MWt would be about 10 MWt , if no reaction from either the reactor operator or the PPS is assumed. The power increase will be less than 10 MWt because in the case being considered the heat exchanger is at least partially bypassed. This bypassing will cause the reactor inlet temperature to increase, with a resulting reduction in reactivity. The power will change over several minutes, a time that is ample for operator action even if all control rods have become inoperative by what amounts to a common failure mode of the rod drives. The safety rods would be unaffected by the event. Figure 9 is a fault-tree diagram for this case.

C. Recommendations

None of the malfunctions of the reactor-cover mechanisms that fall in the Anticipated Fault and Unlikely Fault categories as defined by the RDT Standard can occur if fuel-handling operations are properly terminated before reactor startup. Proper closure of the reactor cover can be assured by utilizing the monitors or the reactor cover in a permissive circuit for reactor startup. Only one event in which the present monitors respond that has significance during reactor operation has been identified--malfunctioning of one or more cover-lock mechanisms during reactor operation. This event has been evaluated as extremely unlikely, with only possible damage to reactor

Fig. 9. Fault-tree Analysis of Malfunctioning of Cover Locks

mechanisms with limited nuclear implication. The only other identified event relevant to this evaluation is overpressure in the outlet plenum without identification of cause. The present reactor-cover monitor will not respond to this event but it would be detected by the monitor for outlet plenum pressure (not part of the FHC monitoring circuit). We therefore recommend that the monitors on the reactor cover be changed to permissive circuits for reactor startup and that the pump trips on these monitoring circuits be bypassed during reactor operation.

VII. MISCELLANEOUS MONITORS IN THE FHC CIRCUIT

A. Description

Monitor circuits in this category are those for the Sequences A and H, the KS2-switch, and instrumented subassemblies.

Sequences A and H include the beginning and terminating operations necessary for unrestricted fuel handling. In Sequence A, the instrumented subassembly and INCOT are raised; control-rod drives are disconnected; the reactor-vessel cover is raised; electrical cables are disconnected; and gripper and holddown mechanisms are prepared for operation. In Sequence H, the plugs and gripper are rotated to "operate" position; the reactor cover is lowered and locked; the holddown mechanism is positioned in the "operate" position; the cover, gripper, and holddown glands are closed; the control-rod drives are secured to control rods; and the platform is positioned in the "operate" position.

The Sequence-A and -H monitors require proper termination of these sequences before the fuel-handling console is de-energized; otherwise reactor startup will be prevented. Once the fuel-handling console is de-energized, these two monitors become passive and remain in an as-is condition, incapable of further reaction. The net effect is that the monitors function in a manner similar to, but not identical with, a permissive circuit for reactor startup. The difference is that a true permissive circuit for reactor startup imposes some condition at the instant of reactor startup, whereas the monitors for Sequences A and H impose a set of conditions at the instant the fuel-handling

console is de-energized, as a prerequisite for later reactor startup. The possibility that the functions monitored by the Sequence-A and-H monitors may revert to an unsafe condition after de-energizing the fuel-handling console before reactor startup has been considered. Most of the functions monitored by these two monitors are passive and require power originating at the fuel-handling console to change their status. However, the reactor-cover-lock mechanisms are exceptions; therefore they are monitored both inside the monitor circuits for Sequences A and H and again in another part of the FHC circuit.

The drive mechanisms for INSAT and INCOT are essentially identical. The circuits monitoring the two mechanisms should, from logical considerations, be similar. Correspondence^{7,8,9,10} on INCOT makes it clear that it is the intent to use these monitors as permissive interlocks for reactor startup. The yoke and position monitors for both the INSAT and INCOT are now connected in series with the Sequence-H reset circuit. Independent INSAT monitors are, in addition, connected in series with the FRD relay circuit whereas the corresponding independent INCOT monitors are connected to operate an alarm only. In this arrangement neither the monitors for INCOT nor INSAT function precisely as permissives for reactor startup.

Three trip circuits now on the INSAT monitor that the following conditions exist before reactor operation: (1) subassembly drive is down, (2) yoke is engaged, and (3) yoke is not retracted. The subassembly drive must be down during reactor operation for normal coolant-flow distribution. The requirement that the yoke be engaged is further assurance that the subassembly is down and cannot be lifted. The second trip circuit on the yoke only reinforces the requirement that the yoke be engaged. The trip circuit for the yoke being engaged specifies a location in which the yoke must be (in) for the reactor to operate. The second yoke-trip circuit specifies a location in which the yoke must not be (out) for the reactor to operate.

The KS-2 switch is a key switch on the fuel-handling console that makes power available for unrestricted fuel handling. It is in the FHC circuit to prevent operation of the unrestricted portion of the fuel-handling console during reactor operation. This function is redundant, because unrestricted fuel handling is possible only if the manual selector switch on the reactor control panel is in the fuel-handling position and if all trip circuits in the fuel-handling trip circuit are closed.

B. Evaluation

All of the trip circuits in the miscellaneous category enforce proper administrative procedure for terminating fuel-handling operations. These trip circuits protect primarily against operator error rather than failure of components or systems. Converting these circuits to permissive circuits for reactor startup provides equivalent enforcement of the procedure. This arrangement would assure that all of the fuel-handling functions monitored by the trip circuits would be properly terminated, at least at the instant of reactor startup. The adequacy of this arrangement has been further evaluated by surveying the possibility that any of the monitored functions may revert to an unsafe condition.

The only reasonable possibility of activating the KS-2 switch during reactor operation is through operator error. However, the consequence of energizing the KS-2 during reactor operation (apart from the tripping the fuel-handling complete circuit) is nil. Such an error on the part of a reactor operator would probably be part of a grosser error in which he attempts to begin full-scale fuel handling while the reactor is in operation. However, this operation is not possible because the fuel-handling circuitry will not respond unless the switch on the reactor-control-room console is in the fuel-handling position and the fuel-handling trip circuit is energized, which are possible only with the reactor shut down. The monitors for Sequence A and Sequence H are in effect permissive circuits for startup, but they too are self-enforcing during reactor operation for the same reason--the reactor must be shut down before fuel handling is possible.

The INSAT mechanism monitored by the FHC circuit can revert to an unsafe condition during reactor operation only if the yoke is withdrawn and the sub-assembly drive is energized to "up". If the INSAT mechanism is properly secured at the instant of reactor startup, the possibility of the mechanism reverting to an unsafe condition is extremely small. By operator error the yoke may be withdrawn but this condition alone is not unsafe. The subassembly must be raised to introduce an unsafe aspect, and power is not available to do so unless the fuel-handling console is energized. The INCOT has a similar mechanical and circuitry arrangement.

C. Recommendations

All of the monitors in the miscellaneous group enforce proper procedure in terminating fuel-handling operations. The possibility that any of the mechanisms may revert to unsafe conditions during reactor operation is extremely unlikely. Therefore, it is recommended that: the monitor circuits be modified to function as permissive circuits for reactor startup only; the KS-2 switch monitor be removed; and the monitors for the INSAT and INCOT drive mechanisms be relocated in the FHC circuit so that the permissive function is enforced at the instant of reactor startup, rather than at the instant of de-energizing the fuel-handling console.

VIII. CONCLUSION

Protection can be provided for all of the fault modes evaluated that are classified as anticipated or unlikely as defined in the RDT Standard by using the existing trip circuits as permissive circuits for reactor startup. The only system fault with possible significant consequences not covered by the permissive circuit is malfunction of the reactor cover-lock mechanism (during reactor operation). Because of the conservative design of the mechanism, such malfunctioning is in the extremely unlikely category as defined in the RDT Standard. The Standard requires that the plant protective system limit the consequence of extremely unlikely faults to a severity level of a Major Incident, which is defined as an occurrence in which damage necessitates replacement or repair of replaceable and semipermanent components or systems. The consequence of a failure of the cover-lock mechanism is probably unaffected by the FHC circuit, either as it exists or as it will be if the recommended circuit modifications are made. Ultimate protection lies with the main-line reactor-shutdown circuits (power, temperature, etc.) The safety rods will remain operable even if this extremely unlikely event is compounded by binding of the control rods.

The pump trips that are designed into the FHC circuit have a valid function for fuel handling but have no identifiable need during reactor operations. The recommended changes would inactivate the FHC-circuit pump trips during reactor operation but would leave them unchanged during fuel-handling operations.

REFERENCES

1. RDT Standard C 16-1T, Supplementary Criteria and Requirements for RDT Reactor Plant Protection Systems, (December, 1969).
2. Upgrading of the EBR-II Plant Protective System - Removal of Flow Related Anticipatory Trip Contacts from the Shutdown Circuit, PM-408, (October 19, 1971).
3. A. V. Campise, R. N. Curran and E. M. Dean, Design Basis Document for Trips Related to Loss of Primary Flow in the EBR-II Plant Protective System (PPS), ANL/EBR-046, (October, 1971) (in publication).
4. A. V. Campise, Technical Rationale and Severity Levels for Dynamic Studies Associated with Deletion and/or Upgrading of the EBR-II Plant Protective System (PPS), ANL/EBR-045 (August 1971) (in publication).
5. A. V. Campise, R. N. Curran, and E. M. Dean, Design Basis Document for Reactivity Change Related Trips in the EBR-II PPS (in the Operate Mode) ANL/EBR-048, (in publication).
6. EBR-II System Design Descriptions: Volume II, Primary System; Chapter 5, Fuel Handling System; Argonne National Laboratory, June 15, 1971 (limited distribution report).
7. Unpublished information, M. Levenson to H. Lawroski and R. K. Winkleblack, January 10, 1972; Subject: INCOT.
8. Unpublished information, W. M. Thompson to O. S. Seim, January 31, 1972; Subject: INCOT Safety Review Recommendation PCS-5-2.
9. Unpublished information, O. S. Seim to M. Levenson, February 2, 1972; Subject: PCS Review of INCOT.
10. Unpublished information, I. Charak to R. K. Winkleblack, February 7, 1972; Subject: INCOT.