Conf-930116--24

Paper to be submitted to American Nuclear Society Probabilistic Safety Assessment '93, Clearwater Beach, Florida, January 26-29, 1993.

Fault Tree Analysis of the EBR-II Reactor Shutdown System

ANL/CP--75950

DE93 004803

by

Sami A. Kamal and David J. Hill

Reactor Analysis Division
Argonne National Laboratory
9700 South Cass Avenue
Argonne, IL 60439
(708) 252-6506

Work supported by the U.S. Department of Energy, Nuclear Energy Programs under Contract W-31-09-ENG-38.

FAULT TREE ANALYSIS OF THE EBR-II REACTOR SHUTDOWN SYSTEM

S. A. KAMAL AND D. J. HILL
Argonne National Laboratory
9700 South Cass Avenue
Argonne, IL 60439
USA

ABSTRACT

As part of the level I Probabilistic Risk Assessment of the Experimental Breeder Reactor II (EBR-II), detailed fault trees for the reactor shutdown system are developed. Fault tree analysis is performed for two classes of transient events that are of particular importance to EBR-II operation: loss-of-flow and transient-over-power. In all parts of EBR-II reactor shutdown system, redundancy has been utilized in order to reduce scram failure probability. Therefore, heavy emphasis is placed in the fault trees on the common cause failures (CCFs) among similar mechanical components of the control and safety rods and among similar electrical components in redundant detection channels and shutdown strings. Generic beta-factors that cover all types of similar components and reflect redundancy level are used to model the CCFs. Human errors are addressed in the fault trees in two major areas: errors that would prevent the automatic scram channels from detecting the abnormal events and errors that would prevent utilization of the manual scram capability. The fault tree analysis of the EBR-II shutdown system has provided not only a systematic process for calculating the probabilities of system failures but also useful insights into the system and how its elements interact during transient events that require shutdown.

INTRODUCTION

The EBR-II core consists of a seven-row hexagonal central core containing enriched uranium. The central core is surrounded by three rows of stainless steel reflectors followed by six-row radial blanket of depleted uranium. EBR-II was originally designed to accommodate twelve control rods in row five of the core subassemblies. These control rods utilize the same type of fuel as the fuel subassemblies except that fewer fuel elements are used. The reactivity control is achieved by moving vertically the control rods within fixed thimbles. The core reactivity is reduced by lowering the fueled portion of the control rods below the core level. Presently, the core has nine high-worth control rods and a single standard-worth rod of the original control rod design. The high-worth control rods utilize the same type of fuel as the standard-worth rods and differ mainly in that the upper shield section of the standard rod is replaced by an absorber follower section. The high-worth rod provides approximately 40% more reactivity worth than a standard-worth rod and thus reactor control can be achieved with fewer number of high-worth rods. The control rod drives are mounted on a platform in a cluster around a central support structure on top of the small rotating plug, see Fig. 1. The control-rod drive shafts, operating through penetrations in the small rotating plug and reactor vessel cover, are connected to the control rods from the top. Each control rod has its own drive, including a release and scram mechanism. During a scram, all the control rods would normally fall (placing the fueled portion of the control rods below the core level) by gravity assisted by pneumatic forces on pistons at the top of the rod drives. In addition to the control rods, reactivity control can be accomplished by two safety rods located in row three of the core region. The two safety rods utilize the same type and quantity of fuel elements as the standard-worth control subassemblies but they have a scram mechanism that is distinctly different from those of the control rods. The two safety rods have a single scram mechanism and are laterally connected so that they can only move together vertically. An important difference between the safety rods and control rods is that the safety-rod drive mechanism, which is connected to the two rods from the bottom, do not pass through the removable reactor-vessel cover. When scrammed, the safety rods fall by gravity assisted by a torsional spring force.

As part of the level I probabilistic risk assessment (PRA) of EBR-II, detailed fault trees for the reactor shutdown system (RSS) are developed.[1] Two classes of transient events that are of particular importance to EBR-II operation and require reactor shutdown are the loss-of-flow (LOF) and transient-over-power (TOP). Normally in these events, detection channels would automatically open a number of contacts in two redundant

shutdown strings. As schematically illustrated in Figs. 2 and 3, elimination of the voltage in the shutdown strings de-energizes electro-mechanical control-power (CP) relays which in turn de-energize the clutches of the individual control rods and thus allow their rapid removal from the core. Reactor shutdown can also be initiated manually by the operators when they push scram buttons that directly open contacts in the two shutdown strings. The operators are instructed to scram first the control rods and if the shutdown can not be verified, the operators should then scram the safety rods. It is noteworthy that the EBR-II shutdown system with its automatic and manual scram capabilities represents the first line of defense against core damage in the event of an LOF or TOP transient. The passive safety features of this liquid-metal reactor (LMR) play an extremely important role in mitigating the consequences of scram failure and as a result, actual core damage would take place only in the event of very severe transients.[1,2]

FAULT TREE DESCRIPTION

Unlike light-water-reactor (LWR) cores, EBR-II is designed such that the reactor core can be shutdown if only a small fraction of its control rods are successfully removed. An additional advantage of EBR-II core design is that it has a control rod drive mechanism that allows only a single control rod to move upward at any given time, thus limiting the amount of reactivity that could be inadvertently inserted.[1] For almost all possible EBR-II core configurations, the reactor can be brought subcritical from any authorized power level by fully removing a single high-worth control rod or the two safety rods. Therefore, a failure to scram in this case would arise only when all the high-worth control rods and also the two safety rods do not drop. As for the very few core configurations that would require two high-worth control rods (the two safety rods are always sufficient) to shutdown the reactor, they can be easily considered once the most probable case is analyzed and the dependence on the number of rods is identified. In the case of the most probable core configuration a failure to scram can occur due to one of three reasons: (i) failure to send a scram signal to the two shutdown strings, (ii) failure to release the control and safety rods, or (iii) failure to remove the control and safety rods. All potential causes and mechanisms that would lead to any of the above failures have been modeled in the LOF and TOP fault trees.

Four of the channels that measure the primary sodium flow in EBR-II core have automatic scram capability. In LOF events, these four flow channels, arranged in a 2-out-of-4 logic, trip both shutdown strings. Two of these channels have magnetic flow-meters and the other two channels utilize pressure difference sensors and transmitters. In addition to the flow sensor each channel includes separate bistables and trip relays for each shutdown string. The channels with pressure difference type of flow sensor require dc power supply components. Three of the flow channels include millivolt-current (MV/I) converters. Each of the flow channel is provided with a high-flow alarm in order to detect false higher-than-normal flow signals that would impede tripping the channel in the event of a low flow condition. In addition to the four automatic scram channels, there are numerous channels that annunciate any malfunction in the two primary pumps.

Automatic plant protection against TOP conditions is provided by three wide-range nuclear channels that have a 2-out-of-3 trip logic in both shutdown strings. Each of the three channels includes a guarded fission chamber detector, preamplifier, high-voltage power supply, two low-voltage power supplies, bistables and trip relays. Each fission chamber detector is placed inside an air cooled thimble that extends from the reactor building operating floor downwards to the reactor core midplane. These channels (to be simply labeled high-flux channels) initiate scram signals if any of the following conditions exist: (i) an increase in neutron flux above the specified set points of 110% of the normal condition, (ii) decrease in the high dc-voltage required for operation of fission chambers, or (iii) non-operate channel condition. The high-flux channels also sound alarms in the control room when the neutron flux exceeds 104%. Because of the numerous shared components between the 110% scram circuit and 104% alarm circuit, the alarm feature has been conservatively ignored in the TOP fault tree. In addition to the three wide-range nuclear channels, there are two linear nuclear channels that provide the reactor operators with an alternative means for power indication.

Figs. 4a and 4b show parts of the fault tree of failure to scram under LOF condition. Similarly, Figs. 5a and 5b show parts of the fault tree of failure to scram under TOP condition. The complete LOF fault tree includes 105 gates and 113 basic events, and TOP fault tree 118 gates and 153 basic events. Both trees are shown in their full extent in Ref. 1. Figs. 4a and 5a show the top events of the two fault trees and illustrate how the trees model the various elements of scram failure. Whereas, Figs. 4b and 5b show some of the basic events and human errors that could lead to scram failure and demonstrate the level of details included in modeling component failures. The triangles in these figures indicate transfers to other parts of the fault trees. The top event in Fig. 4b addresses the failure of low-flow channel LPPF, which utilizes electro-magnetic flow sensor, to open its three contacts in shutdown string A. The top event in Fig. 5b addresses the failure of high-flux channel B to open its two contacts in shutdown string A. This portion of the TOP fault tree covers failures of components which are used to detect the high flux (HF) and components which monitor the drop in voltage (LV) to the neutron detectors. The two RSS fault trees differ mainly in the way the scram signal is initiated and voltage in the two shutdown strings is eliminated. The two trees are similar with regard to modeling the release and removal of the control and safety rods.

In addition to the low-flow and high-flux channels, there are also four subassembly outlet temperature (SOT) channels that have automatic scram capability in the event of core

overheating. Accordingly, the SOT channels provide a redundant and diversified automatic scram capability in the event of an LOF or TOP. The SOT channels scram has a 2-out-of-4 trip logic in both reactor shutdown strings. The thermocouples used in the SOT channels are located in the reactor vessel upper plenum above driver assemblies where they sense the sodium temperature as the coolant exits these assemblies. The modeling of the SOT channels covers the failure to initiate an automatic scram signal in terms of the failures of the electrical components and a human error in setting the trip points of all the channels. This SOT branch is then combined through an AND-gate (gate No. R0240 in Fig. 4a) with the failure to initiate a scram signal by the low-flow channels in the LOF fault tree. In the TOP fault tree the SOT branch is combined with the failure to initiate a scram by the high-flux channels (gate No. R0540 in Fig. 5a). CCFs between similar components in different types of automatic scram channels are considered in the fault trees.

COMPONENT FAILURE DATA

Component failure data from three different main sources have been gathered and compared before deciding on the data set to be used in the RSS fault tree calculations. The three sources are: (i) EBR-II specific data, (ii) LMR CREDO data,[3] and (iii) LWR generic data from more than one source.[4,5] The plant specific data, which are the preferred data source whenever they are available, are found to be limited and have to be supplemented with data from the other two sources. Data used in the RSS fault trees are generally of two forms; one based on failure rate per hour of standby (h) and the other based on failure per demand (d). When the component failure is described in the first form, the component test interval is provided along with the failure rate. Electro-mechanical relays, which subsequently are found to have a large effect on the RSS failure probability, have been given special attention. Two distinct failure modes are postulated for each relay and its set of contacts. One failure mode, which may be described as "relay armature fails to move from closed to open position" has an occurrence rate of 2.0×10^{-7}/h. This failure rate is derived from plant specific data and is supported by generic relay data. The other failure mode, "relay contacts fail closed," has an occurrence probability of 3.0×10^{-4}/d based on generic relay data, although this mode has not been detected during plant operation.

An important part of the failure data of standby components such as those in the RSS is the interval between tests that reveal component failures. The operability of the low-flow channels is checked during reactor startup and every week during steady power operation. In this operability test, the channel response to an actual increase in reactor flow is confirmed and also channel capability to trip at the specified set point when a signal simulating the flow is gradually reduced. The capabilities of the high-flux channels and the SOT channels to trip are checked as part of the reactor startup procedure for each reactor run (100-day duration in present analysis). Also checked as part of the startup procedure are: (i) the trip logic of the various types of channels to initiate automatic scram in each shutdown string and (ii) rod drop time of each control rod without pneumatic force assistance. Every day during reactor operation, each control rod is moved a short distance and then returned back to its original position. This daily exercise of the rods enables the reactor operators to detect any potential rod binding. Also during reactor operation, readings are taken every four hours for critical core parameters, including those of the scram channels of low-flow, high-flux, and SOT.

COMMON CAUSE FAILURES

In order to reduce scram failure probability redundancy has been utilized in all parts of the EBR-II RSS; different types of detection channels, two shutdown strings, multiple control-power relays on the two shutdown strings, and different drive mechanisms for the control rods and safety rods. As a result, CCFs of similar components rather than independent failures are expected to dominate the probability of scram failure, and accordingly heavy emphasis is placed on modeling all possible CCFs in the RSS fault trees. Ideally, the numerical values of the parameters to be used in the selected CCF model should be estimated in a manner that maximize the use of plant specific event data. This would include data screening, classification, and analysis as well as developing uncertainty distributions and point estimate of the CCF model parameters.[6] However, due to virtually non-existent common cause events in the EBR-II recorded data, such a detailed data analysis becomes impossible and one has to consider data from the more extensive operating experience of LWR components.

The CCF model used in the RSS fault trees is based on the beta-factor method which requires a single common cause parameter in addition to the individual component failure probability. An underlying assumption in this CCF model is that whenever a common cause event occurs all the redundant components in the group fail together. This assumption is not considered very restrictive since any group of redundant components in the EBR-II RSS fails only when a large fraction of its components fail. In the present fault tree analysis, the beta-factor method is taken one step further by using generic beta factors that reflect the redundancy level in the group. A generic beta factor of 0.100 is used for redundant components numbered less than four, 0.020 for redundant components numbered four or five, and 0.008 for redundant components numbered six or more. These generic beta factors are selected based on comparison between the failure probability of redundant components as obtained by the present method and the more precise multiple greek letter (MGL) method.[1]

HUMAN ERRORS

Human errors are addressed in the fault trees in two general areas: latent errors that would prevent the automatic scram channels from detecting the abnormal transient events and errors

that would prevent utilization of the manual scram. Human errors in the first area include errors in calibrating the electrical components, in setting the specified trip points, and in performing channel operability tests. Pre-startup interlock checks provide recovery paths from setting incorrectly the trip points of the low-flow and high-flux channels and thus the associated human errors become very small.[7] The potential for common errors in performing each of the above tasks has been taken into account. Such a common human error is found to be the dominant failure mode, with a probability of 2.5×10^{-2}, in the case of the SOT channels. A simple procedural change that adds a sign-off step for the checker would reduce significantly the probability of setting the trip temperatures too high.

In the second area, two human tasks are considered: (i) reactor operators scramming the reactor when the automatic scram signal fails, and (ii) reactor operators scramming the safety rods when the control rods fail to drop for mechanical reasons. With regard to the first task, the approach taken in estimating the human error probability is that the operators should be able to diagnose the abnormal transient condition and realize the need to initiate a scram based on parameters unaffected by the automatic scram failure. If the operators in this situation fail to scram the control rods, they will also fail to scram the safety rods. The probability of failing to perform this task is estimated at 0.05 in the event of an LOF and 0.10 in the event of a TOP based on a screening analysis of post-accident tasks. It is important to point out that determining the probabilities of these two human errors accurately would require extensive effort that involves consideration of different transient scenarios and a range of time-available for the operators to initiate a scram. Subsequent sensitivity analysis of core damage frequency,[1] however, has shown that further refinement of the screening values is not warranted. As for the second task, a more detailed human reliability analysis shows that the operators in this situation will be aware of the need to scram and they will likely follow the manual-scram emergency procedure. The probability of failure to perform this task is estimated to be 7.5×10^{-3} which is a small probability compared to the failure to scram the control rods.

ANALYSIS RESULTS

The ANL EBR-II PRA Codes Package[1] is used to draw the fault trees, determine the minimal-cut-sets, calculate top event probability, and perform uncertainty analysis. Table 1 gives the probabilities of scram failure in case of an LOF or TOP. The table provides the mean probabilities (point-mean with uncertainty coupling of similar components that have the same probability distribution curve) of scram failure along with its three main causes; the signal failure, mechanical failure, and CP-relays failure. The signal part represents the failure to send a scram signal to the shutdown strings by automatic scram channels and manual scram as well. For both the LOF and TOP events, the results are shown with and without the automatic scram capability of the SOT channels. Although in both types of events the SOT channels are expected to provide a redundant automatic scram capability, the signal failure results are separated in order to illustrate some important aspects of channel redundancy. The SOT scram capability reduces slightly the failure probability of the LOF signal from 4.24×10^{-7} to 1.74×10^{-7} since there are similar components in the low-flow channels and SOT channels and the signal failure is determined in this case by the CCFs among these similar components. There is however a more distinct reduction in the case of TOP from 1.64×10^{-4} to 4.55×10^{-6}. With no similar components in the high-flux and SOT channels, the two types of channels become fully independent. The difference between the signal failure probability in the two cases without the SOT channels (i.e. 4.24×10^{-7} for LOF versus 1.64×10^{-4} for TOP) is attributed largely to the difference in the test intervals. The low-flow channel components are tested for trip operability every 7 days; whereas the high-flux channel components are tested every 100 days, prior to each reactor run.

The second potential cause of scram failure consists of the failure to release or remove all the control rods and the two safety rods as well. This part of scram failure, which is labeled mechanical failure, has a fixed probability of 2.26×10^{-7}/d in all the cases shown in Table 1 with the major portion of it relates to the inability of the control and safety rods to move within their thimbles. The two types of rods have the same subassembly and thimble design and are supplied with coolant from the same plenum and as a result one can postulate a common cause failure that would affect the two types of rods. The advantage of having the safety rods is underscored when one considers the mechanical failures of the RSS with and without the safety rods. The probability of the control rods mechanical failures, including the magnetic clutches failure to disengage and rods binding due to reactor vessel cover tilting is estimated at 3.5×10^{-6}/d. But when one considers that this failure can be overcome by manually scramming the safety rods with an associated human error probability of 7.5×10^{-3}, these mechanical failures of the control rods (excluding the CCF among the control and safety rods) contribute only 2.6×10^{-8} to the overall scram failure probability.

The third and final potential cause of scram failure is the failure of the CP-relays to open their contacts. In the original RSS design and in subsequent modifications, particular consideration has been given to possibility of CP-relay failures and therefore multiple relays have always been provided. There are presently five CP-relays on the two shutdown strings with any one of these relays capable of de-energizing the clutches of at least four control rods. There are also two additional CP-relays either of which can de-energize the clutch of the safety rods. The CCFs among all the seven relays are estimated to have a probability of 4.32×10^{-6}/d in all the cases listed.

It is very important when one evaluates and compares the probability of scram failure to consider the frequency and severity of the transients that require scram in the first place.

According to the EBR-II PRA accident sequence analysis,[1] the frequency of all LOF transients is about 1.0 per year whereas the frequency of all TOP transients is only 0.04 per year. As a result, the frequency of LOF transients without scram becomes about 4.7×10^{-6} per year and for TOP transients without scram 3.6×10^{-6} per year. With regard to the severity of the transients, it was found that because of EBR-II passive safety features, less than 0.5% of the LOF transients and about 8% of the TOP transients would actually lead to a widespread core damage in the event of a scram failure. The corresponding core damage frequencies are 2.23×10^{-8} per year for LOF transients 2.94×10^{-8} per year for TOP transients. The large remaining percentage of LOF and TOP transients either do not cause any core damage or cause damage that is limited to few subassemblies. The above frequencies underscore the extremely low probability of core damage as a result of scram failure in the event of an LOF or TOP transient. These low frequencies also show that the EBR-II RSS and passive safety features provide excellent protection against scram failure.

CONCLUSIONS

- Fault tree analysis of EBR-II shutdown system provided a systematic process for calculating the probability of scram failure. The RSS fault trees were subsequently integrated in accident sequence analysis and core damage calculations. EBR-II scram failure probabilities of 4.72×10^{-6} per demand in event of an LOF transient and 9.10×10^{-6} per demand in event of a TOP transient are reasonably low. When combined with low initiating frequencies and the core accident-mitigating features, the severe core damage frequencies become extremely small, 2.23×10^{-8} per reactor year as a result of LOF transients and 2.90×10^{-8} per reactor year as a result of TOP transients.

- In all parts of the EBR-II RSS, redundancy has been utilized and thus common cause failures among redundant and similar components become the dominant modes of failures in the shutdown system. The RSS fault trees adopted a CCF model which was based on the beta-factor method. This CCF model which was applied to all types of redundant components was found to be useful in approximately but consistently representing common mode failures particularly among components for which CCF parameters could not be extracted from their operating records.

- The fault tree analysis of scram failure also provided a means for understanding and delineating the RSS and how its various elements function and interact during abnormal transient events. This was particularly evident in the two crucial areas of manual scram initiation and role of safety rods as a redundant shutdown mechanism.

ACKNOWLEDGEMENTS

This work was supported by the U.S. Department of Energy, under Contract No. W-31-109-ENG-38. The authors would like to thank Nelson Hanan, of ANL Engineering Physics Division, for his valuable suggestions and comments during fault tree development; Jordi Roglans, of ANL Reactor Analysis Division, for explaining how to utilize the PRA Codes Package; Lynn Christensen, of ANL EBR-II Division, for explaining the intricacies of the RSS circuits; Pete Davis, of PRD Consulting, for his valuable comments on the common cause modeling; and Donald Schurman, of Science Applications International Corporation, for permitting the use of his Human Reliability Analysis results.

REFERENCES

1. D. J. Hill et al., EBR-II Level 1 Probabilistic Risk Assessment, Argonne National Laboratory, Volume I, Final Draft, Revision 2 (June 1991).

2. "The experimental Breeder Reactor-II Inherent Safety Demonstration," Nuclear Engineering and Design, 101, Entire Issue (April 1987).

3. K. H. Koger et al., "The Centralized Reliability Data Organization (CREDO) Assessment of Critical Component Unavailability in Liquid-Metal Reactors," Nuclear Technology, 85, 251-257 (June 1989).

4. "IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Power Generating Stations," IEEE Std 500-1984.

5. M. L. Roush et al., Integrated Approach Methodology: A Handbook for Power Plant Assessment, SAND87-7138, Sandia National Laboratories (1987).

6. A. Mosleh et al., Procedures for Treating Common Failures in Safety and Reliability Studies, NUREG/CR-4780, Vols. 1 and 2, Prepared for U.S. NRC and EPRI by PLG (January 1989).

7. A. D. Swain and H. E. Guttmann, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, NUREG/CR-1278, Prepared for U.S. NRC by Sandia National Laboratories (August 1989).

TABLE 1. SCRAM FAILURE PROBABILITY (PER DEMAND) FOR LOF AND TOP EVENTS

Type of Failure	LOF Event		TOP Event	
	Flow Channels Only	Flow Channels and Temp. Channels	Flux Channels Only	Flux Channels and Temp. Channels
Automatic and Manual Signals	4.24×10^{-7}	1.74×10^{-7}	1.64×10^{-4}	4.55×10^{-6}
Mechanical	2.26×10^{-7}	2.26×10^{-7}	2.26×10^{-7}	2.26×10^{-7}
Control-Power Relays	4.32×10^{-6}	4.32×10^{-6}	4.32×10^{-6}	4.32×10^{-6}
SCRAM TOTAL	4.97×10^{-6}	4.72×10^{-6}	1.69×10^{-4}	9.10×10^{-6}

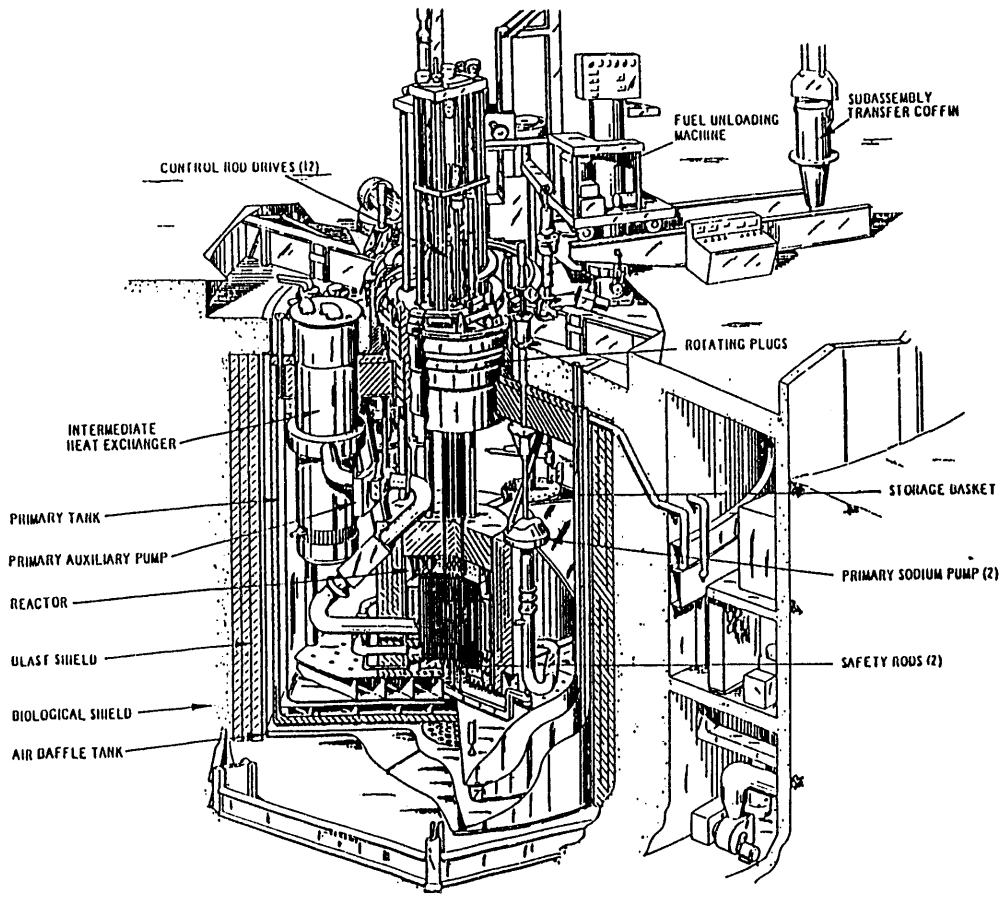

FIGURE 1. EBR-II CORE AND SURROUNDING COMPONENTS.

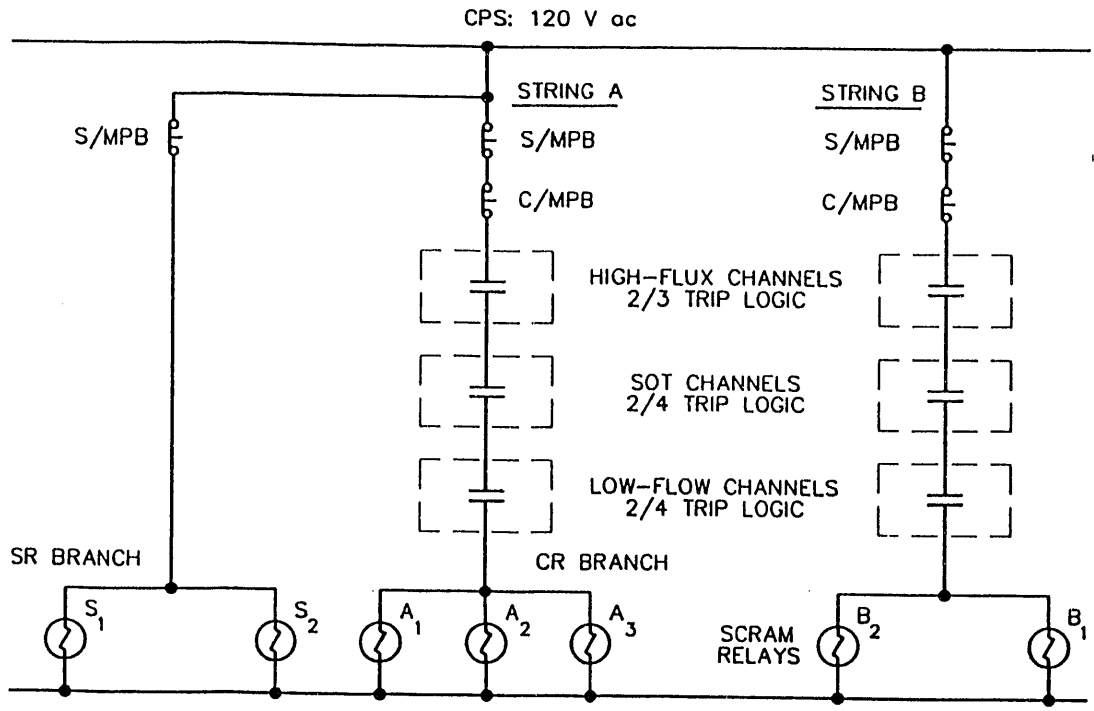

FIGURE 2. SIMPLIFIED SCHEMATIC OF EBR-II SHUTDOWN STRINGS

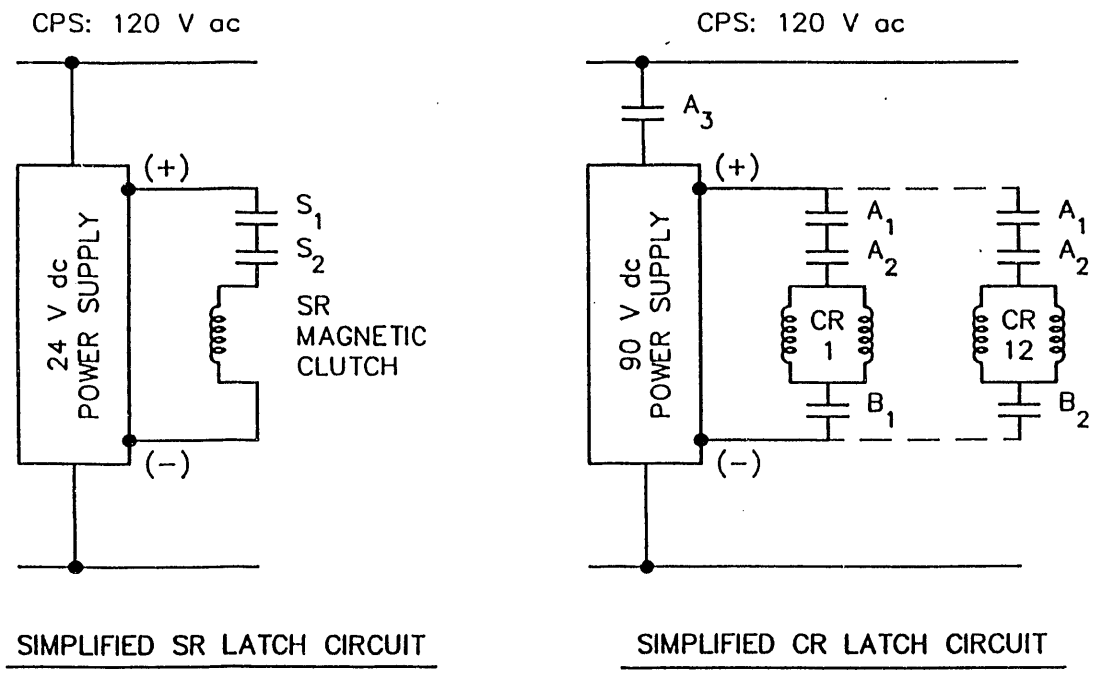

FIGURE 3. SIMPLIFIED LATCH CIRCUITS OF CONTROL RODS AND SAFETY RODS

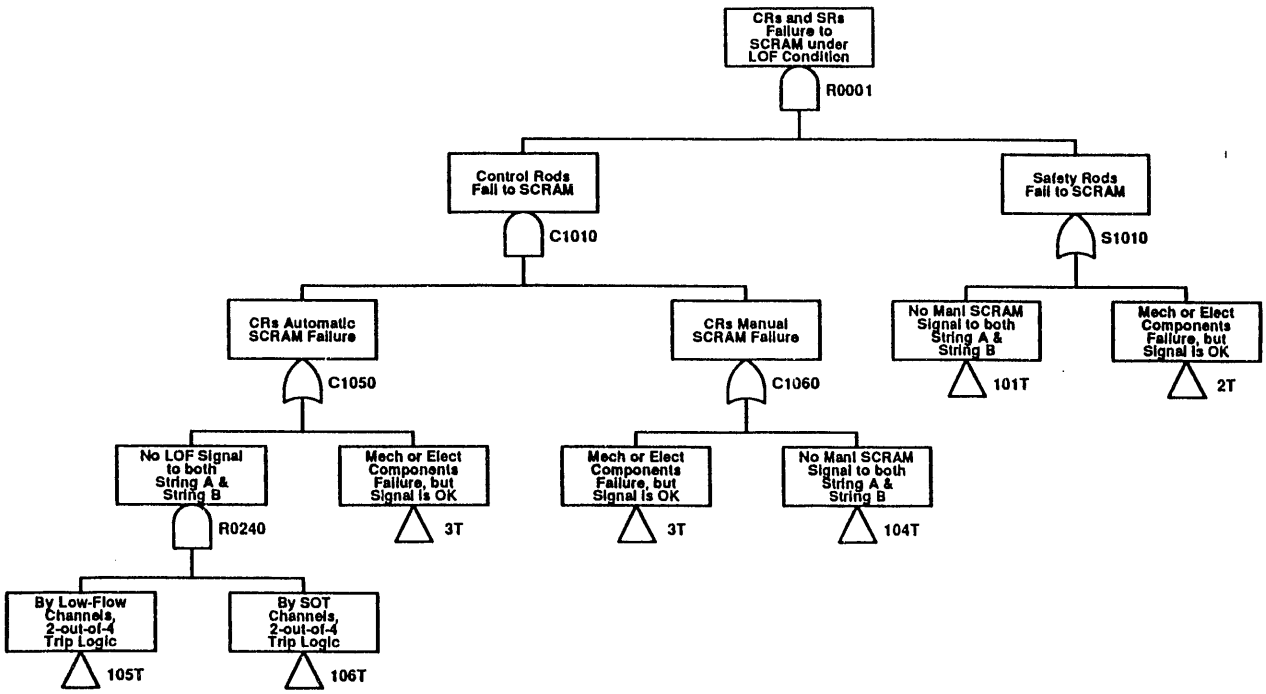

FIGURE 4a. PART OF FAULT TREE OF FAILURE TO SCRAM UNDER LOF CONDITION SHOWING TOP EVENT

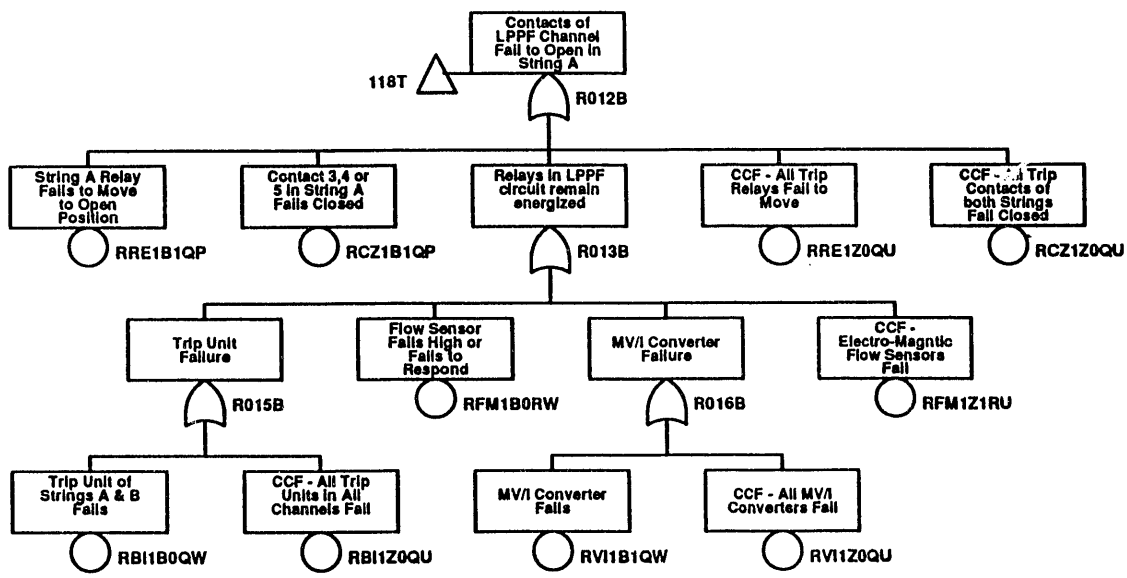

FIGURE 4b. PART OF FAULT TREE OF FAILURE TO SCRAM UNDER LOF CONDITION SHOWING SOME OF COMPONENT FAILURES

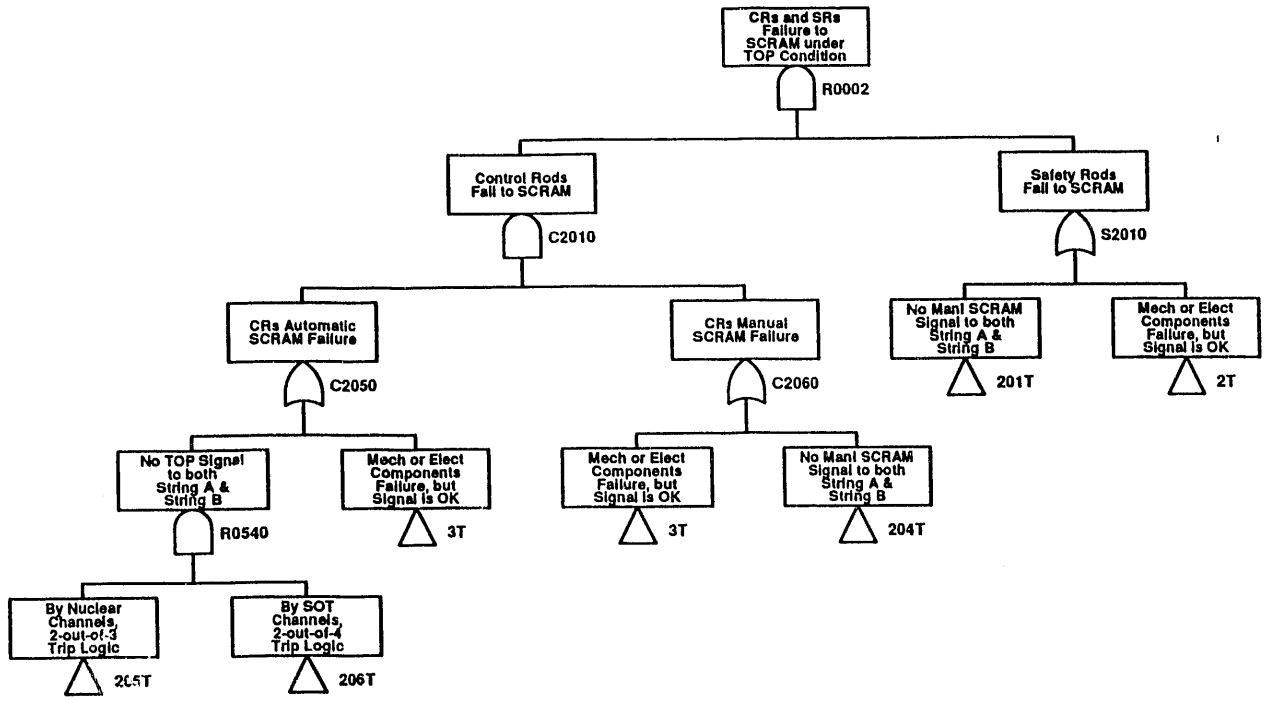

FIGURE 5a. PART OF FAULT TREE OF FAILURE TO SCRAM UNDER TOP CONDITION SHOWING TOP EVENT

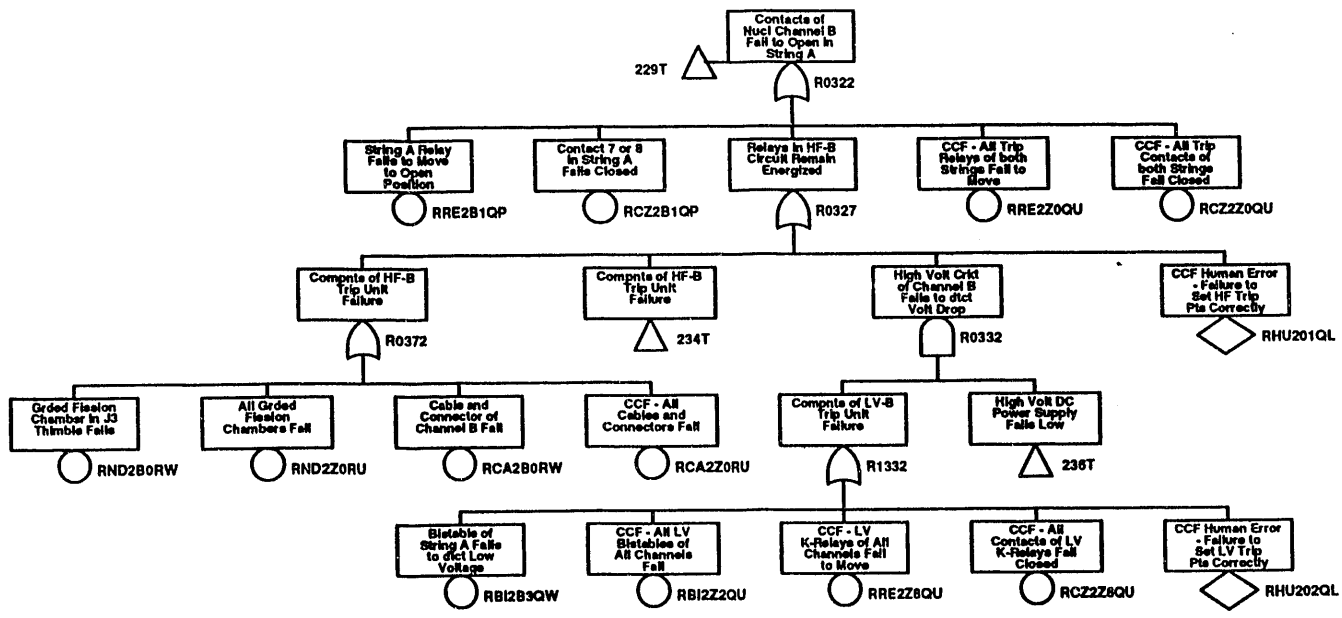

FIGURE 5b. PART OF FAULT TREE OF FAILURE TO SCRAM UNDER TOP CONDITION SHOWING SOME OF COMPONENT FAILURES AND HUMAN ERRORS

END

DATE
FILMED
5/05/93