RELIABILITY ANALYSIS OF THE PROTECTION SYSTEM OF IEA-R1m BRAZILIAN RESEARCH REACTOR CONSIDERING THE MODIFICATION PROJECT TO UPGRADE REACTOR POWER LEVEL TO 5MW

PATRÍCIA PAGETTI DE OLIVEIRA
Institute for Nuclear and Energetic Research
São Paulo, Brazil

ABSTRACT

The objective of this paper is to present the reliability of the IEA-R1m Reactor emergency shutdown protection function. The fault tree methodology has been utilized and primary event reliability data is based on generic information obtained from databases. The unreliability of the systems involved in the emergency shutdown protection function of IEA-R1m Reactor is quantified for a 120-hour period of continuous operation and it is expressed as the probability of failure on demand, considering two different accident scenarios.

1 INTRODUCTION

Pool-type research reactors have the potential of a broad spectrum of risks ranging from a minor activity release to a major catastrophic core meltdown. The reactor shutdown protection function is a vital barrier in almost all of the accident sequences to prevent the releases to the environment and save the public from high radiation doses. For this reason, the reliability analysis presented in this paper has been utilized as an important support document to the Safety Analysis Report of the plant, which was developed to comply with the requirements of licensing by the National Atomic Energy Authority, named CNEN (Brazilian Nuclear Energy Commission), in view of the modification project to modernize the reactor and upgrade its power.

This paper aims to present the results obtained in the Reliability Analysis of the IEA-R1m Reactor Emergency Shutdown ("SCRAM") Protection Function. The IEA-R1 is a pool type, light water cooled and moderated, and graphite reflected research reactor. The reactor building is located in the limits of IPEN (Institute for Nuclear and Energetic Research), in the *campus* of the University of São Paulo, Brazil. Although designed to operate up to 5 MW, IEA-R1m reactor was being operated at 2 MW since early fifties. In the beginning of 1995, IPEN has developed a modification project to modernize and upgrade the power of the IEA-R1 from 2 MW to 5 MW and to increase its operational cycle from 8 h day, 5 days a week, to 120 h continuous per week. On November of that year, the reactor started operating in continuous periods of 64 hours per week. The upgrading process of the reactor was concluded in 1997, when the reactor has completed 40 years, and the name was changed from IEA-R1 to IEA-R1m (modified).

The project of upgrading the IEA-R1 reactor from 2 MW to 5 MW required a general revision of the various existing systems which resulted in changes in some of the systems, replacement of some structures, and introduction of new systems, with a view to ensure adequate safety of the reactor. In particular, some improvement has been conducted in the

Reactor Protection System and in the safety related instrumentation. New interlocks were conceived into 2 out of 3 logic, specifically to drive primary circuit isolation and emergency core cooling system valves using pool level signals as initializing events. Interlock to protect core against power excursion at lower power level has also been designed. Nuclear measuring channels and control rod drivers remain unchanged, being scope of future works. After power upgrading, plant modernization will follow with the substitution of all nuclear instrumentation and control room.

The Reliability Analysis of IEA-R1 Reactor "SCRAM" Function has been conducted already considering all the changes in systems configurations. The fault-tree methodology has been utilized and primary event reliability data was based on generic information obtained from databases. The unreliability of the subsystems involved in the shutdown protection function of IEA-R1 research reactor is quantified for 120-h period of continuous operation, having in mind two different accident scenarios. One of these scenarios was related to an accident initiating event of insertion of excess reactivity in the reactor core and the other one was characterized as a loss of reactor coolant accident. The unreliability of the IEA-R1m Reactor "SCRAM" Function was expressed as the probability of failure on demand.

2 DESCRIPTION OF THE SYSTEMS INVOLVED IN THE IEA-R1m REACTOR "SCRAM" FUNCTION ([1] and [3])

The reactor shutdown function is intended to lead the reactor to subcriticality, inserting negative reactivity of at least 1$ (~ 763 pcm). More specifically, the reactor "SCRAM" is the reactor emergency shutdown protection function, which is intended to terminate rapidly the neutron chain reaction whenever reactor safety limits are exceeded. At the 5 MW power level, the shutdown of the reactor must be done through the insertion of 3 out of 4 neutron absorber control and safety rods in the core.

The systems involved in the reactor emergency shutdown protection function are described below.

<u>Reactor Protection System (RPS)</u>

The function of the RPS is to automatically initiate the operation of the system responsible for the negative reactivity insertion in the reactor core when any violation of the plant safety condition has been detected. The RPS includes part of the Nuclear Instrumentation Subsystem (NISs), which is used to monitor and to transmit the signal to indicate abnormal power level or period of the reactor. The RPS also includes the Reactor Trip Circuit (RTC), which compiles the information obtained from the NISs and from other safety related instrumentation and actuates the Reactivity Control System (RCS), which has to accomplish the negative reactivity insertion in the core.

The RPS includes all the instruments used to monitor plant safety parameters and which are designed to detect the abnormal operating conditions requiring the shutdown of the reactor. This includes the nuclear instrumentation channels, which belong to the Nuclear Instrumentation Subsystem (NISs), that are used to monitor and control reactor power level and period. Among the nuclear instrumentation channels used to trip the reactor, three of them are operating in the power region which starts from the 10 percent of nominal power (Safety Channels 1, 2 and 3). These channels are calibrated to actuate the RCS, in a 2 out of 3 logic, when an abnormal power level of 105 percent of nominal power has been achieved.

The RPS also includes the field sensors or safety related field instrumentation that monitors other safety related process variables, alarms, annunciators, indicators as well as system manual actuation devices. Among the field instrumentation important to plant safety it can be mentioned the pool level sensors, which present an important contribution in the reliability quantification of the reactor shutdown protection function considering the occurrence of a LOCA.

The Reactor Trip Circuit (RTC) is composed mainly by electromechanical relays used to implement the RPS logic.

Reactivity Control System (RCS)

The RCS is intended to keep the reactor within specified operational limits as well as to accomplish the reactor shutdown when it is necessary. The components of the RCS that are responsible for the reactor shutdown are 4 neutron absorber control and safety rods. One of these elements have a control function and the other three have a safety function. There is no redundant system for the RCS in the IEA-R1m reactor.

The reactor shutdown signal is generated by the interruption of the electrical current (opening the RTC relays contacts) that energizes the magnets which couple the safety and control rods to its respective drivers mechanisms.

The IEA-R1m Reactor "SCRAM" Functional Block Diagram is presented in **Figure 1**.

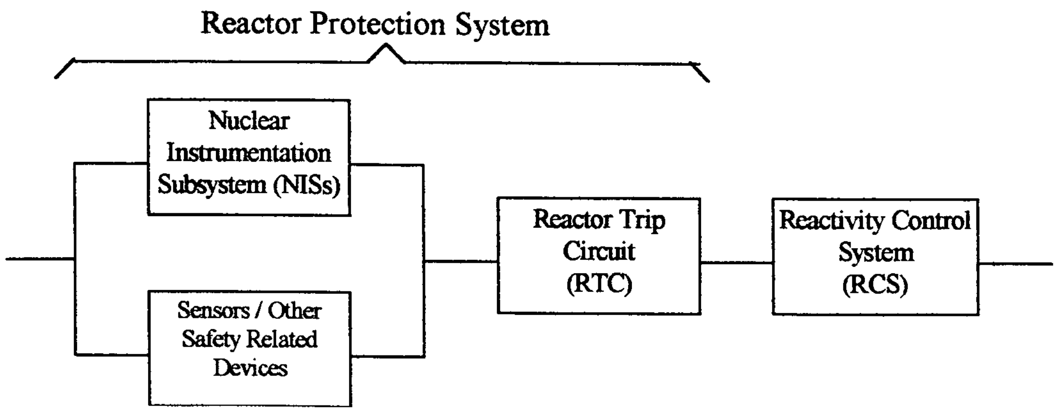


Figure 1. Functional Block Diagram of the IEA-R1m Reactor "SCRAM" Function

The diagrams presented in **Figures 2 and 3** are originated from Figure 1, showing some details of the IEA-R1m Reactor "SCRAM" for the two accident conditions considered in this paper.

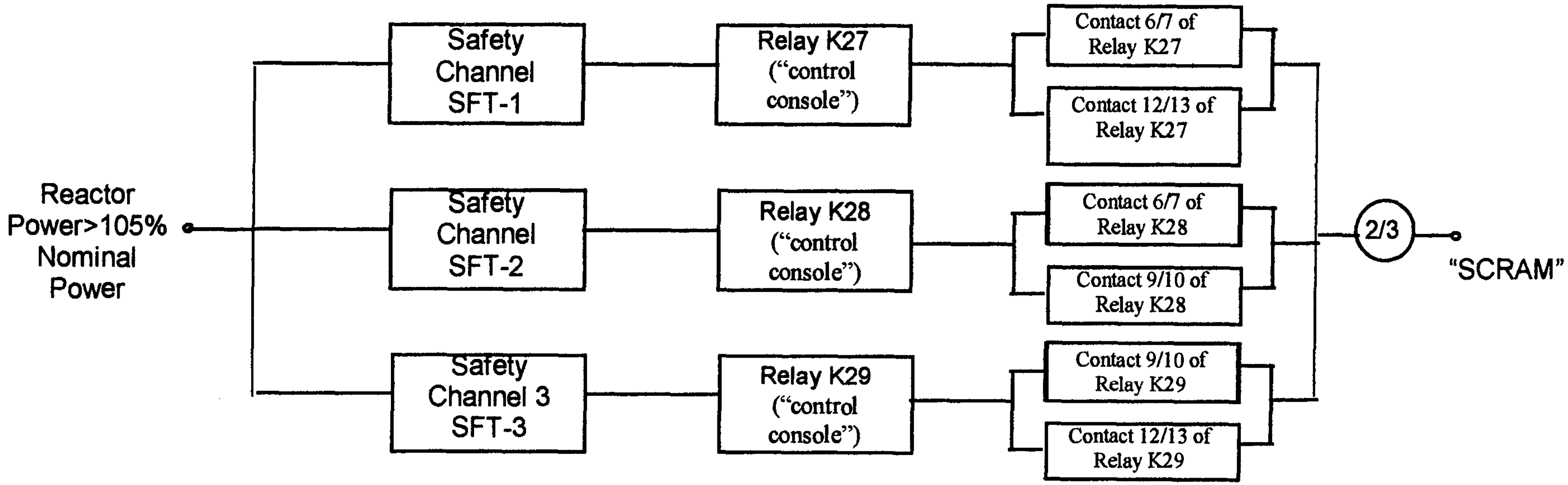
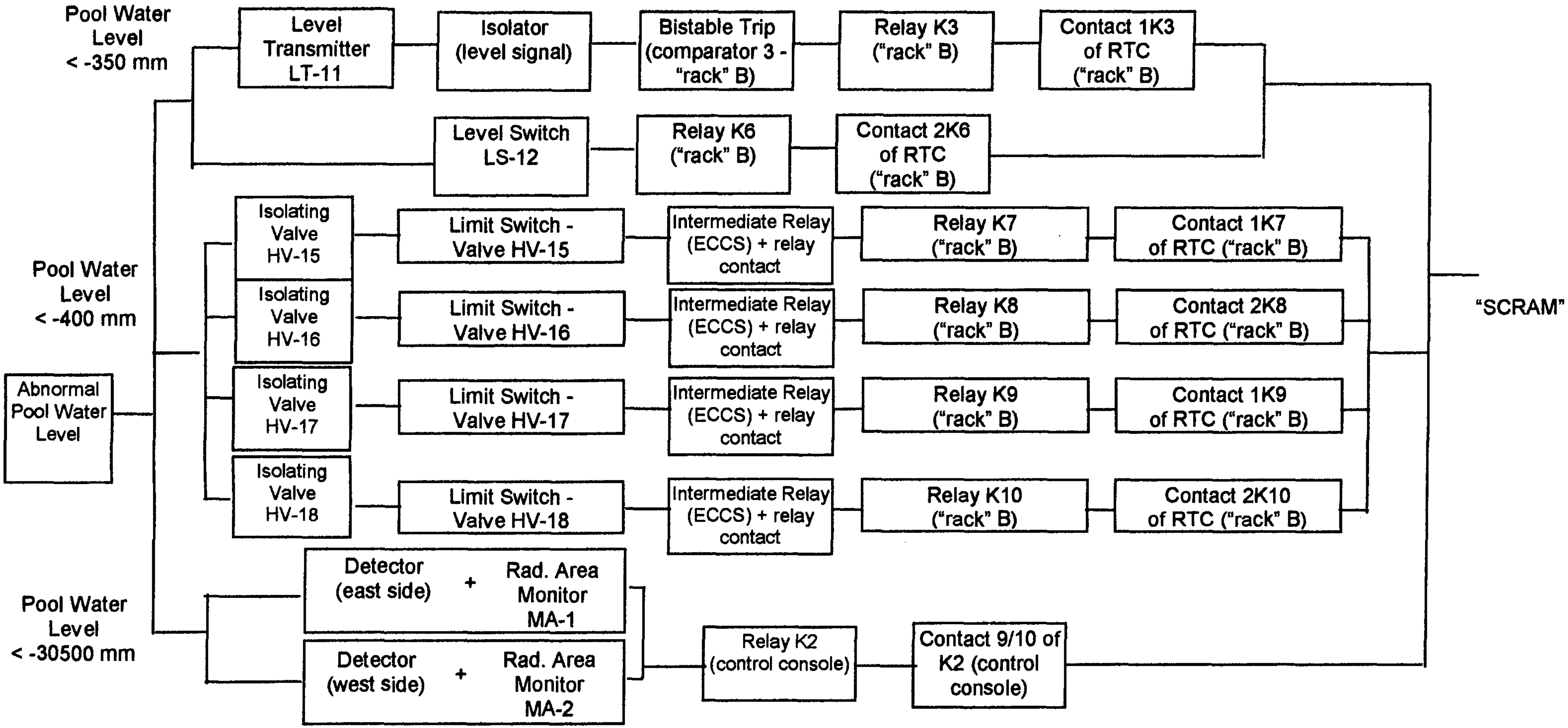


Figure 2 Functional Block Diagram of a "Simplified Circuit" of the Reactor Protection System for the Accident Condition of Excess Reactivity Insertion



RTC : Reactor Trip Circuit
ECCS : emergency Core Cooling System

Figure 3 Functional Block Diagram of a "Simplified Circuit" of the Reactor Protection System for the Accident Condition of Loss of Reactor Coolant

3 RELIABILITY ANALYSIS OF THE IEA-R1m REACTOR "SCRAM" FUNCTION

The reliability analysis of IEA-R1m emergency shutdown protection function concentrated on evaluating the probability of failure to "SCRAM" event considering a demand originated from one of two different accident conditions. Firstly, it has been considered an abnormal power condition, characterizing an insertion of excess reactivity event. Secondly, it has been assumed an abnormal pool level condition, indicating the occurrence of a loss of coolant accident.

Basic Assumptions

The following functional assumptions are made for plant operation in this analysis:

(a) During the normal operation of the reactor, for power levels greater than 10 percent of nominal power, safety channels are energized and continuously monitoring reactor power. Reactor Trip Circuit relays and the magnets of the Reactivity Control System which couple safety and control rods to its respective driver mechanism are also energized.

(b) With the upgrading of power to the 5 MW level, the reactor is expected to be in operation 5 days per week continuously, i.e., in 120-hour cycles.

(c) The manual actuation of the "SCRAM" function can be accomplished by the operator by pushing the "SCRAM BAR" installed in the central panel of the control console, actuating simultaneously all the neutron absorber rods.

(d) Maintenance activities like inspections, functional tests, repairs and calibration are always performed with the reactor in a shutdown condition.

Failure to "SCRAM" Fault Tree

The analysis has been developed using the fault tree methodology, which is based in a graphical model to represent the failure propagation logic related to a system or a safety function, as shown in **Figure 4**. In this case, the fault tree *top event* has been defined as *"Failure of the IEA-R1m Reactor SCRAM given that a plant safety condition has been violated"*.

The fault tree from which the results of this study were obtained was constructed from the reactor design documentation, upgrading project documentation and from the IEA-R1m Reactor Safety Analysis Report ([1] and [3]). The model covers electronic, electrical and mechanical components of the systems described in section 2 above and which could interfere in the reactor "SCRAM" success. The model considers events representing independent failures and events corresponding to multiple failures originated by common cause failures. Human failures in the calibration of nuclear instrumentation channels and in recognizing the necessity of a manual actuation of the "SCRAM" function have been considered in the model. Loss of the Electrical Power supplies has not been considered in the analysis since it implies in the automatic actuation of reactor shutdown function, characterizing a fail-safe condition.

Statistical Assumptions

The following statistical assumptions have been adopted in this analysis :

(a) Fault tree primary events are independent.

(b) The unreliability of various components was based on an exponential model, for a mission time of 120 hours. Therefore, it is assumed that at every new mission the components are "as good as new". It was also assumed that all failures are immediately detectable and there are no undetectable failures.

(c) The components involved in the reactor "SCRAM" function have not suffered aging effects during the last 40 years of IEA-R1m operation. This hypothesis is based on the fact that safety and control instruments operate in adequately controlled environment conditions, minimizing component degradation.

(d) A conservative value of human error corresponding to the probability of failure in manually actuating the reactor "SCRAM" was assumed to be 1 . This value was adopted due to the lack of more realistic information from the operating personnel of the plant.

(e) Following the simplified approach suggested in WASH-1400 Report [4], the contribution of common cause failures was evaluated by including special events in the fault tree model. Each event was considered as having a probability of occurrence calculated from a log-uniform uncertainty distribution, considering that the lower limit represents the optimistic situation of total independence of the events and the upper limit represents totally dependent events.

(f) Failure data for all the components was obtained from a generic data source [2], allowing the quantification of all primary events of the fault tree model developed in this analysis.

Fault Tree Quantification

Table 1 contains input data, obtained from the generic data source [ ], used in the quantification of the IEA-R1m Reactor "SCRAM" Function Fault Tree. The values presented in the column named *Component Failure Rate / Probability of Failure on Demand* correspond to the mean of the uncertainty distribution indicated in this data source.

The final results obtained in the analysis are reported in **Table 2**. In this case, the unreliability of the Reactor "SCRAM" Function is equivalent to its probability of failure on demand, and it has been derived, by hand calculations, as a function of the unreliability of the various items involved in its implementation, considering an operation cycle of 120 continuous hours.

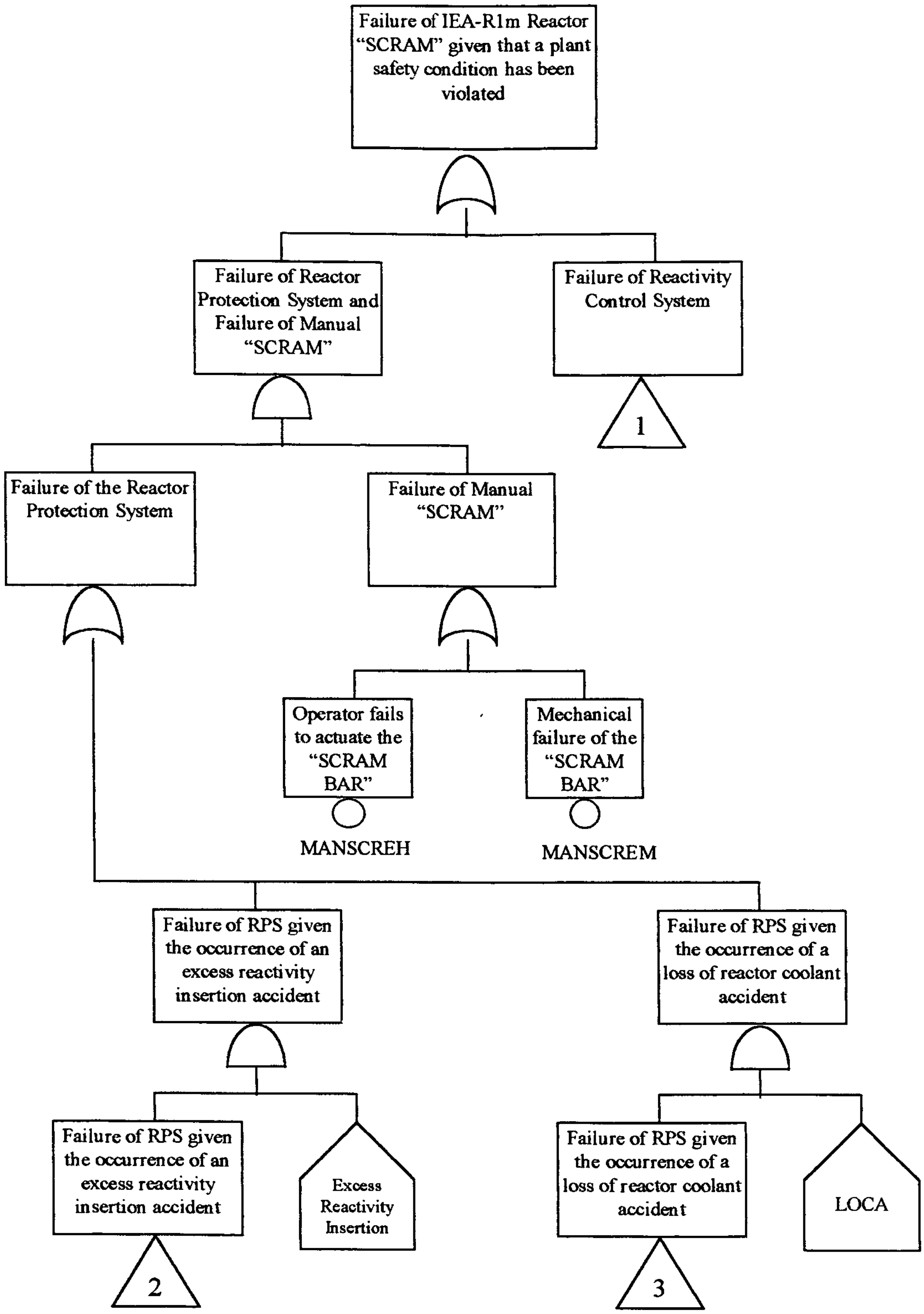


Figure 4 IEA-R1m Reactor "SCRAM" Fault Tree (sheet 1/6)

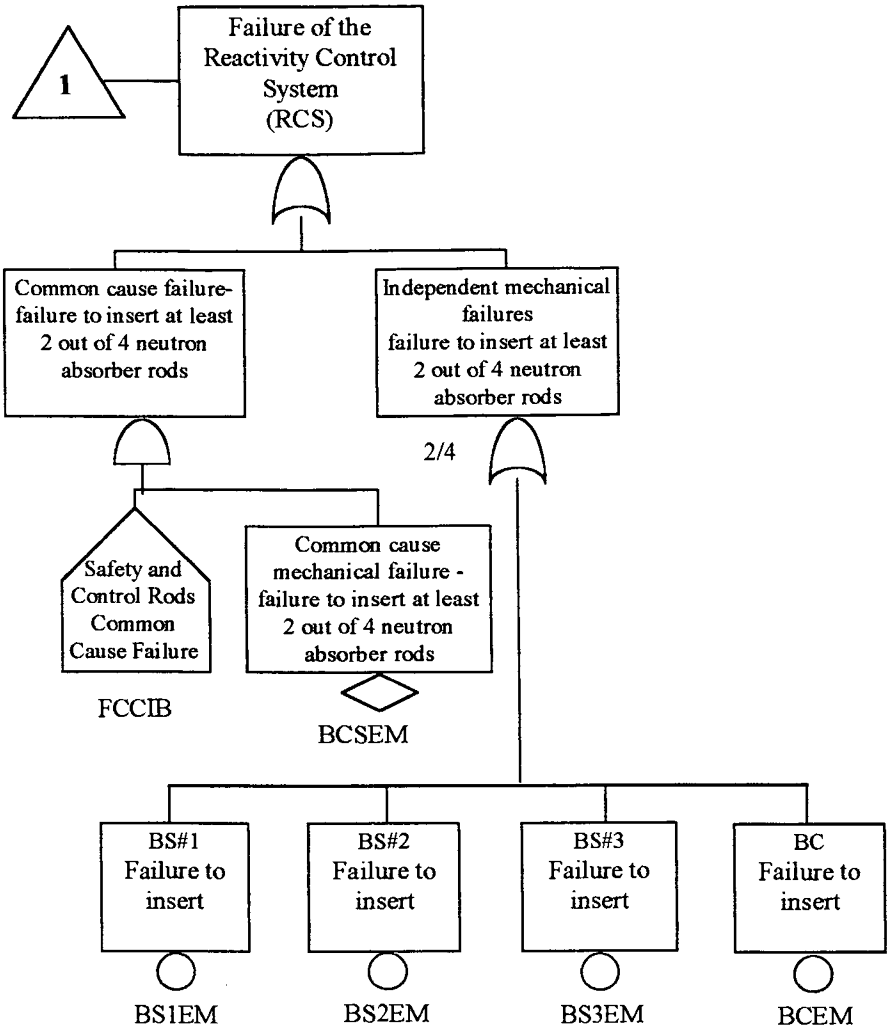


Figure 4 IEA-R1m Reactor "SCRAM" Fault Tree (sheet 2/6)

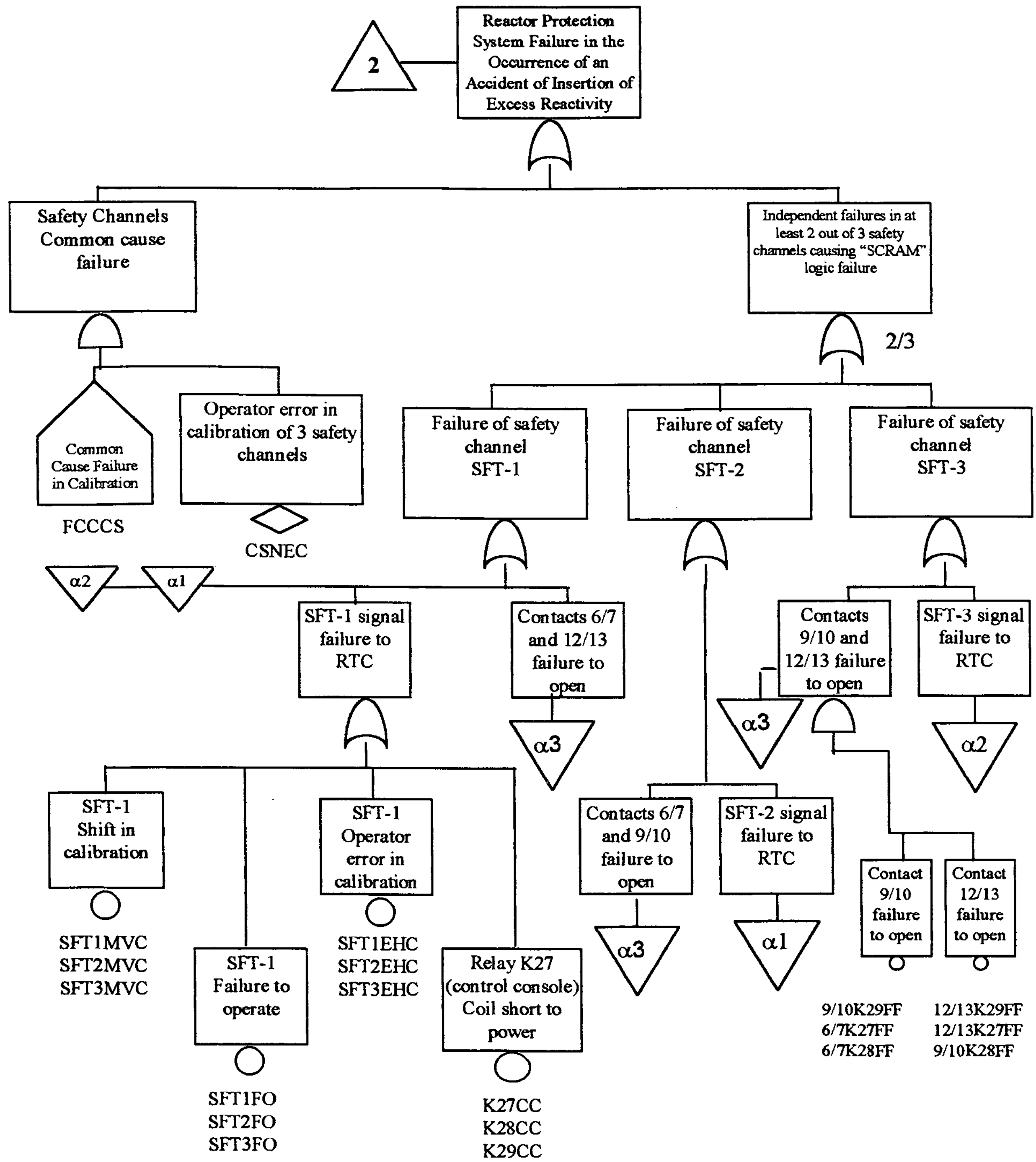


Figure 4 IEA-R1m Reactor "SCRAM" Fault Tree (sheet 3/6)

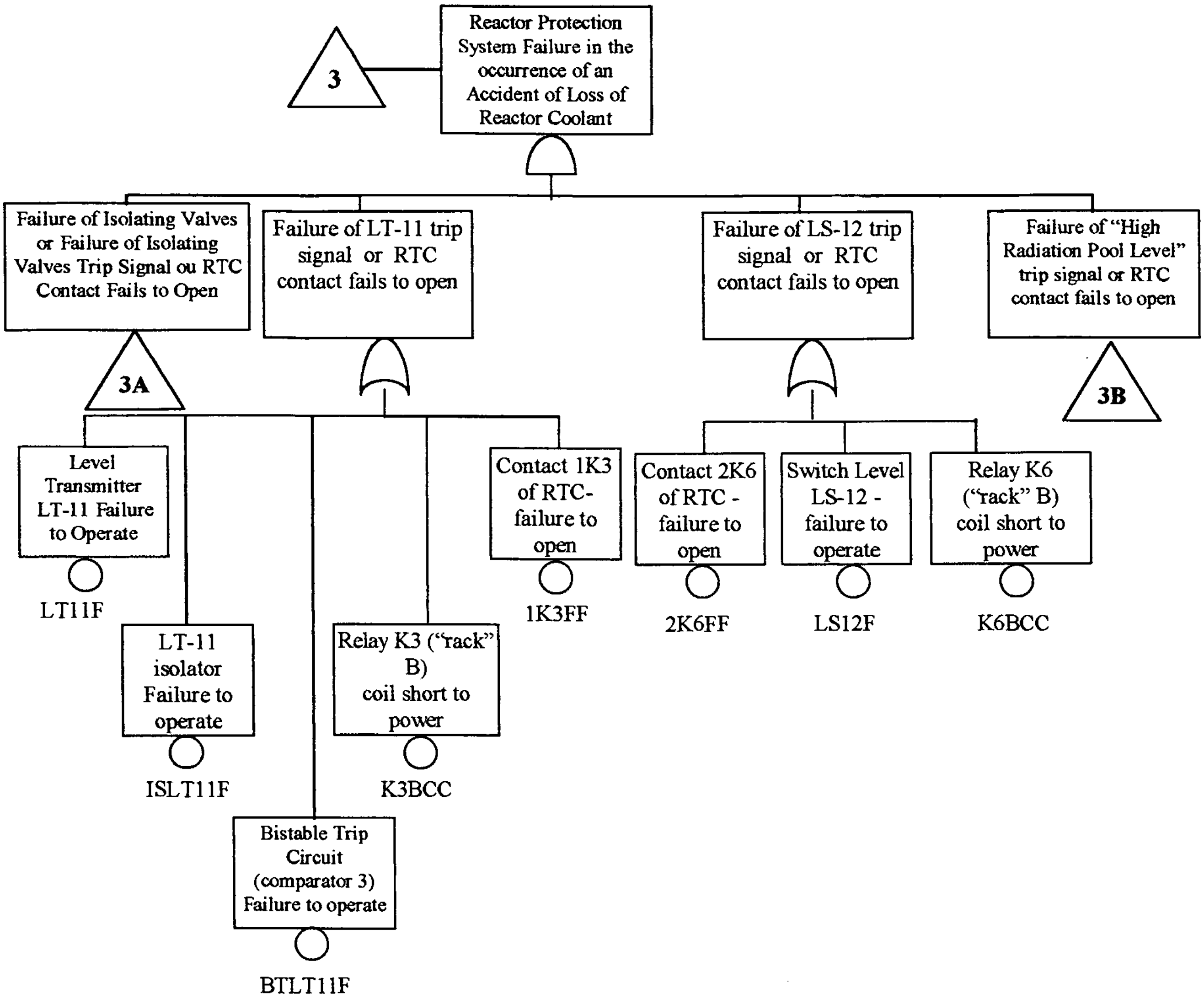


Figure 4 IEA-R1m Reactor "SCRAM" Fault Tree (sheet 4/6)

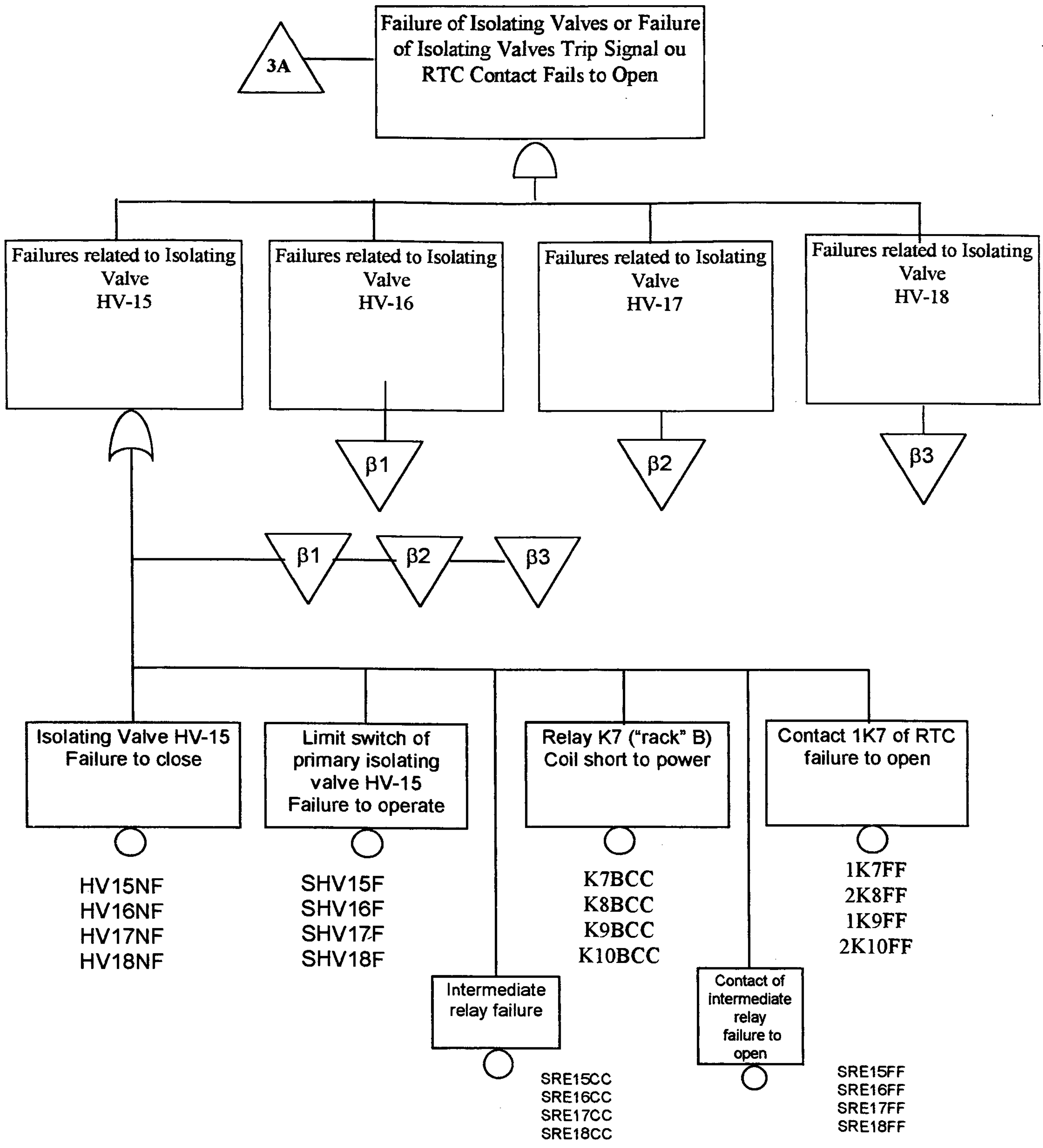


Figure 4 IEA-R1m Reactor "SCRAM" Fault Tree (sheet 5/6)

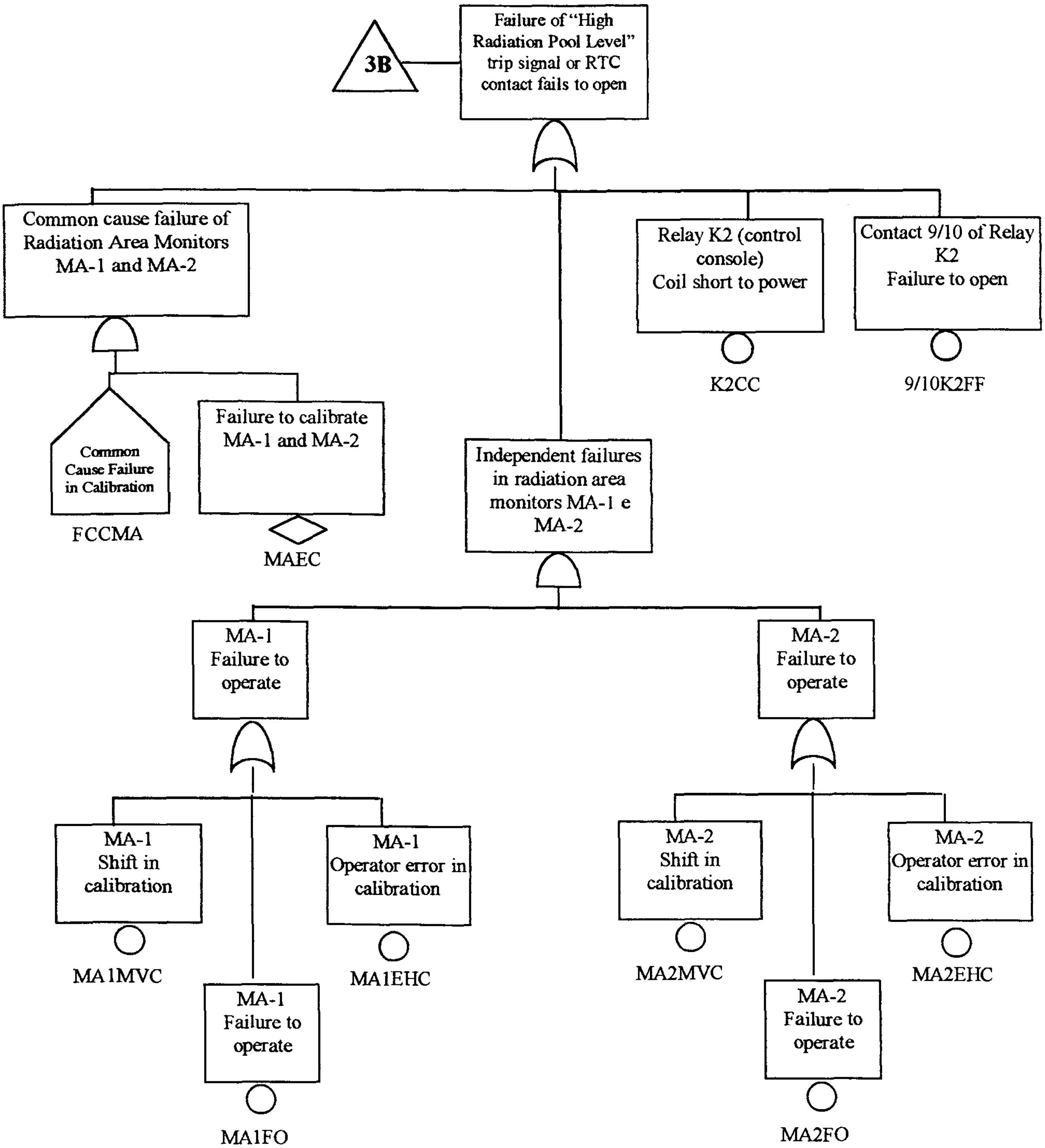


Figure 4 IEA-R1m Reactor "SCRAM" Fault Tree (sheet 6/6)

TABLE 1 Component Failure Data Used as Input Data to the Fault Tree Model of the IEA-R1m Reactor "SCRAM" Function ([2] e [4])

Component	Failure Mode	Primary Events [a]	Failure Rate/ Failure Probability [b]	Unreliability in a 120-hour Period
Safety and Control Rods	Failure to insert – mechanical failure	BS1EM; BS2EM; BS3EM; BCEM	$1{,}2 \times 10^{-4}$ /d	$1{,}2 \times 10^{-4}$
	Common cause mechanical failure – at least 2 out of 4 rods fail to insert	BCSEM	$1{,}7 \times 10^{-5}$ /d	$1{,}7 \times 10^{-5}$
	Operator fails to actuate the SCRAM BAR (human error)	MANSCREH	1,0	1,0
Safety Channels	Shift in calibration	SFT1MVC; SFT2MVC; SFT3MVC	$8{,}0 \times 10^{-5}$ /h	$9{,}6 \times 10^{-3}$
	Failure to Operate	SFT1FO; SFT2FO; SFT3FO	$2{,}7 \times 10^{-6}$ /h	$3{,}2 \times 10^{-4}$
	Operator error in calibration	SFT1EHC; SFT2EHC; SFT3EHC	$1{,}2 \times 10^{-3}$ /d	$1{,}2 \times 10^{-3}$
	Common Cause Failure – Operator Error in calibration of the 3 safety channels	CSNEC	$9{,}0 \times 10^{-5}$ /d	$9{,}0 \times 10^{-5}$
Relay / Relay Contacts	Coil short to power	K2CC; K27CC; K28CC; K29CC; K3BCC; K6BCC; K7BCC; K8BCC; K9BCC; K10BCC;SRE15CC; SRE16CC; SRE17CC; SRE18CC	$2{,}7 \times 10^{-8}$ /h	$3{,}2 \times 10^{-6}$
	Failure of normally closed contacts to open, given not energized	9/10K2FF; SRE15FF; SRE16FF; SRE17FF; SRE18FF; 1K3FF; 2K6FF; 1K7FF; 2K8FF; 1K9FF; 2K10FF;6/7K27FF; 12/13K27FF; 6/7K28FF; 9/10K28FF; 9/10K29FF; 12/13K29FF	$5{,}3 \times 10^{-7}$ /d	$5{,}3 \times 10^{-7}$

a. These codes correspond to the primary events in the fault tree model of Figure 4.
b. Mean values are given as probability of failure on demand (/d) or failure rate per hour (/h).

TABLE 1 Component Failure Data Used as Input Data to the Fault Tree Model of the IEA-R1m Reactor "SCRAM" Function ([2] e [4])

Component	Failure Mode	Primary Events [a]	Failure Rate / Failure Probability [b]	Unreliability in a 120-hour Period
Radiation Area Monitor	Shift in calibration	MA1MVC; MA2MVC	$8{,}0 \times 10^{-5}$ /h	$9{,}6 \times 10^{-3}$
	Failure to operate	MA1FO; MA2FO	$2{,}7 \times 10^{-6}$ /h	$3{,}2 \times 10^{-4}$
	Operator error in calibration	MA1EHC; MA2EHC	$1{,}2 \times 10^{-3}$ /d	$1{,}2 \times 10^{-3}$
	Common Cause Failure – Operator Error in calibration of both radiation area monitors	MAEC	$1{,}8 \times 10^{-4}$ /d	$1{,}8 \times 10^{-4}$
Level Transmitter	Failure to operate	LT11F	$1{,}4 \times 10^{-6}$ /h	$1{,}7 \times 10^{-4}$
Level Switch	Failure to operate	LS12F	$3{,}0 \times 10^{-8}$ /d	$3{,}0 \times 10^{-8}$
Isolator	Failure to operate	ISLT11F	$1{,}7 \times 10^{-6}$ /h	$2{,}0 \times 10^{-4}$
Bistable Trip Circuit (comparator)	Failure to operate	BTLT11F	$1{,}0 \times 10^{-6}$ /h	$1{,}2 \times 10^{-4}$
Primary Isolating Valve	Failure to close	HV15NF; HV16NF; HV17NF; HV18NF	$7{,}2 \times 10^{-3}$ /d	$7{,}2 \times 10^{-3}$
Limit switches of primary isolating valves	Failure to operate	SHV15F; SHV16F; SHV17F; SHV18F	$3{,}7 \times 10^{-4}$ /d	$3{,}7 \times 10^{-4}$
SCRAM BAR	Common Cause Failure- Mechanical failure of the 4 push-button type switches	MANSCREM	$3{,}5 \times 10^{-7}$/d	$3{,}5 \times 10^{-7}$

a. These codes correspond to the primary events in the fault tree model of Figure 4.
b. Mean values are given as probability of failure on demand (/d) or failure rate per hour (/h).

TABLE 2 Results of the Reliability Analysis of the IEA-R1m Reactor "SCRAM" Function

	Unreliability of the Reactor "SCRAM" Function in a 120-hour Period
Insertion of Excess Reactivity Accident	$4,7 \times 10^{-4}$
Loss of Reactor Coolant Accident	$1,7 \times 10^{-5}$

4 CONCLUSIONS AND FINAL REMARKS

In this study the quantified unreliability of the IEA-R1m Reactor SCRAM Function has been derived in terms of the unreliability of components of the Reactor Protection System and of the Reactivity Control System. The results are of preliminary nature as it depends upon the quality of input data. However, these had shown to be very useful in the critical understanding of the failure mechanisms related to the reactor "SCRAM". The values obtained can be considered satisfactory since they are compatible with the probability of failure of typical reactor shutdown systems, as referenced in [2]. Operational records of the IEA-R1m Reactor from 1957 to 1997 show that the systems responsible for the implementation of the reactor SCRAM Function have never failed to accomplish the required function, demonstrating an efficient and reliable operation during all these years. This fact is then confirmed by the results obtained for the reactor operation at the 5 MW power level.

Finally, the following suggestions are made for improving the existing systems and for performing further work on the PSA of IEA-R1m Research Reactor:

(a) Use of generic reliability data for a specific application is a difficult task and even questionable. Concerning to operational records, there is a question whether the data are representative samples of the equipment behavior or the records accurately meet the failure modes, and whether the recorded performance of the equipment and the new application are comparable. Also, there is the question of whether the maintenance and operational regimes are sufficiently similar.

(b) Anyway, there is a need for generic data on failure rates for research reactor components, to be used in preliminary PSA studies.

(c) Concerning common cause failure contribution, the application of other analysis techniques such as the Beta Factor method, Multiple Greek Letters Factor and other Markovian alternatives could be developed when reactor operational data become appropriate to be used in PSA. Furthermore, a better understanding of common mode failure data for research reactors is needed.

(d) To perform aging studies for the IEA-R1m reactor components and incorporate these models in the reliability calculations of the systems or safety functions.

(e) Routine quality assurance activities concerning maintenance, calibration, tests, inspections, etc. must be emphasized with respect to their importance in improving plant safety.

(f) Human factor database is needed for risk assessment of the research reactors.

(g) Validation of the PSA studies for research reactors is very important. However it depends upon good documentation requiring important assumption and decision to be properly recorded during design and operation of a research reactor.

(h) Because of the fact that relevant data on research reactors is lacking for PSA of the research reactors, an effective exchange of the information should be made among research reactor's community.

5 REFERENCES

[1] IPEN-CNEN/SP. **IEA-R1m Safety Analysis Report,** September, 1996.

[2] IAEA-TECDOC-478. **Component Reliability Data for Use in Probabilistic Safety Assessment**, Vienna, 1988.

[3] GENERAL ATOMIC. **E-115-403 Instrumentation System Operation and Maintenance Manual**, March, 1975.

[4] U.S. NRC. **Reactor Safety Study: an Assessment of Accident Risks in U.S. Commercial Nuclear Plants,** WASH-1400 (NUREG-75/014), 1975.

[5] MOSLEH, A., FLEMING,K., PARRY,G., PAULA,H., WORLEDGE,D., AND RASMUSON,D., **Procedures for Treating Common Cause Failures in Safety and Reliability Studies - Procedural Framework and Examples, NUREG/CR-4780, EPRI NP-5613, PLG-0547, Vol.1**, January, 1988.

Parte 10 texto completo ✓

IPEN/CNEN-SP
BIBLIOTECA
"TEREZINE ARANTES FERRAZ"

Formulário de envio de trabalhos produzidos pelos pesquisadores do IPEN para inclusão na Produção Técnico Científica

---

AUTOR(ES) DO TRABALHO:

PATRÍCIA DA SILVA PAGETTI DE OLIVEIRA

LOTAÇÃO: RES **RAMAL:** 9438

TIPO DE REGISTRO:

art. / periód.:	☐	Publ. IPEN	☐	. resumo	☐
cap. de livro	☐	Art. conf	☒	outros (folheto, relatório, etc...)	☐

TITULO DO TRABALHO:

RELIABILITY ANALYSIS OF THE PROTECTION SYSTEM OF IEA-R1m BRAZILIAN RESEARCH REACTOR CONSIDERING THE MODIFICATION PROJECT TO UPGRADE REACTOR POWER LEVEL TO 5 MW

APRESENTADO EM: (informar os dados completos - no caso de artigos de conf., informar o título da conferência, local, data, organizador, etc..)

"IAEA TECHNICAL COMMITTEE MEETING ON RESULTS AND STATUS OF PSA APPLICATIONS AND TOOLS" ; THE HAGUE, NETHERLANDS , 21 - 25 JUNE 1999
(organizado pela Agência Internacional de Energia Atômica)

PALAVRAS CHAVES PARA IDENTIFICAR O TRABALHO:

RELIABILITY ANALYSIS ; PROTECTION SYSTEM ; RESEARCH REACTOR

ASSINATURA: Patricia Oliveira

DATA: 21 / 02 / 2000

6719