NUKLEONIKA 2005;50(3):105–112

ORIGINAL PAPER

Improving reactor safety systems using component redundancy allocation technique

Aziz Shafik Habib,
Hoda Abd-el Monem Ashry,
Amgad Mohamed Shokr,
Azza Ibrahim Dakhly

Abstract This paper addresses the improvements to the reliability of the safety systems of nuclear reactors using redundancy allocation technique. The study has been carried out using the Probabilistic Safety Assessment (PSA). PSA involves, among others, the use of fault and event tree tools in the evaluation of the safety system failure probabilities and the quantification of annual occurrence probability of the accidental conditions postulated in the design of the nuclear reactors. The PSA has been presented and discussed. The Egypt Second Research Reactor, ETRR-2, has been used as a case study. The failure probability of the already existing safety systems has been reviewed. The effect of the allocation of more redundant components to the existing safety systems on the failure probability of the systems has been evaluated. The event trees for two selected initiating events, from those events postulated in the ETRR-2 design, have been studied considering the allocation of more redundant components to the safety systems. The result of the study showed that further improvement could be introduced to the reliability of the Confinement Ventilation System (CVS).

Key words redundancy allocation • risk management • safety systems • probabilistic safety assessment • ETRR-2

A. S. Habib
Department of Mathematics,
Faculty of Science,
El-Minufiya University,
Shibeen El-koom, El-Minufiya, Egypt

H. A. M. Ashry, A. I. Dakhly✉
National Center for Radiation Research
and Technology,
Atomic Energy Authority,
Cairo, Egypt,
Tel.: +202/ 4040174, Fax: +202/ 28876033,
E-mail: azdakhly@yahoo.com

A. M. Shokr
Atomic Energy Authority, ETRR-2,
13759, Abou zabal, Egypt

Received: 14 July 2004
Accepted: 4 May 2005

Introduction

One of the main concerns about the nuclear reactors is safety. For a nuclear reactor to be licensed, the reactor design should demonstrate that the technical objectives for the reactor safety are fulfilled. These technical objectives are [6]:

- to ensure the general prevention of accidents with high confidence margi;
- to ensure that, for all accidents taken into account in the design, even those of very low probability, the radiological consequences, if any, would be minor, and
- to ensure by prevention, protection, and mitigation measures that severe accidents with significant radiological consequences are extremely unlikely.

In order to ensure that these technical safety objectives are fulfilled, an a-priori overall safety analysis of the reactor is requested. It is a common practice that the available probabilistic tools, such as fault and event trees, are used for this analysis. This analysis should demonstrate, among others, that the reliability of the reactor safety systems is higher than pre-established values. Furthermore, the tendency in the reactor safety

design is to continuously improve the safety, which requires improvements of the reliability of the reactor safety systems. Redundancy is one of the design principles that are applied to ensure and continuously improve the reliability of reactor safety systems. Redundancy implies multiplicity, that is, important components and systems are installed in greater numbers than would be necessary for normal system or component operation [5].

The purpose of this work was to review the reliability of the safety systems of the research reactors using the redundancy allocation technique, and to study the effect of allocating redundant components on the safety systems reliability. The Egypt Second Research Reactor, ETRR-2, has been considered as a study case.

Probabilistic Safety Assessment (PSA)

In order to verify that the reactor fulfills public acceptance criteria for licensing of research reactors, accident sequences that contribute to the reactor risk are identified and the radiological consequences that could affect the public and the operators are assessed.

PSA quantifies the probabilities and consequences associated with accidents and malfunctions by applying probability and statistical techniques as well as the consequences of evaluation method. PSA examines all pertinent information available and widens the historical basis by using data from actual events in combination with logic models to predict the frequencies and consequences of events which have not happened but which could be causes by accidents. Modern PSA embraces the event/fault tree analysis tools, computer models, reliability theory, system analysis, human interaction analysis, probability theory and statistics [3]. These and the traditional engineering disciplines (mechanical, electrical, structural, chemical, and nuclear) are integrated into a formal process that addresses the two components of risk: likelihood of these scenarios and their consequences.

One can think in terms of the basic four-element process as displayed in Fig. 1.

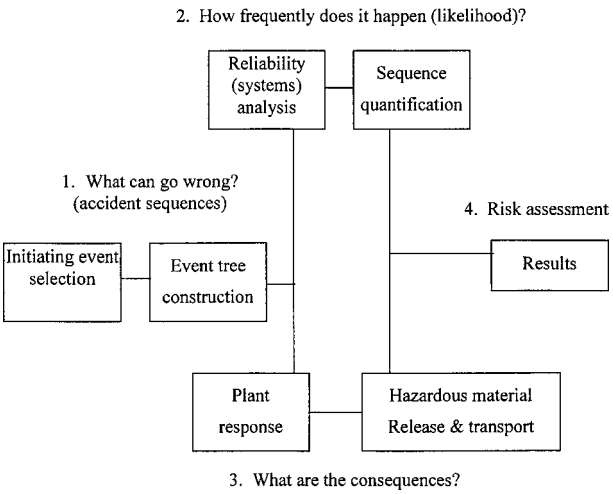

Fig. 1. Basic elements of PSA methodology.

The first three elements provide answers to the most fundamental safety questions, whereas the fourth element, the risk assessment, provides displays of results in the form suitable for the decision making process.

Various methods and models have been developed for system reliability analysis. The method, which is most frequently used within the framework of PSA, is known as fault tree analysis. This method has been used extensively in nuclear, chemical, aerospace and defense industries. The fault tree is a logic model of various parallel and sequential combinations of faults that could result in the occurrence of the predefined undesired events, e.g., the "top event" of the fault tree. The faults can be events that are associated with infrequent hardware failures, human interactions or other events leading to the undesired event. A fault tree thus depicts a logical inter-relationship of basic events that leads to the undesired top event.

Accident initiating events are those events that could initiate an accident scenario. For PSA applications, initiating events of the nuclear reactor are grouped according to the similarity of their impact on the integrity of the reactor as well as regarding performance of the set of protective actions designed to deal with the occurrence of events [4]. Event trees are inductive logic models, which display a possible accident sequence from a given specific accident initiating event.

ETRR-2 safety and safety-related systems

The Egypt Second Research Reactor, ETTR-2, is an open pool type research reactor. The reactor nominal power is 22 MW with a maximum thermal neutron flux of 2.7×10^{14} n/cm^{-2} s^{-1}. Several experimental devices are installed at the reactor so that it can be used for radioisotope production, basic and applied research in science and engineering, material testing, neutron radiography, neutron activation analysis, and for training [1]. The reactor coolant and moderator is light water and the reflector is beryllium. The reactor uses U_3O_8-Al plate type fuel with Al cladding and 19.75% enrichment. Several safety and safety related systems are installed at the reactor. These systems are designed to detect, control, and mitigate the effect of initiating events postulated by the reactor safety analysis.

These systems include:

1. First Shutdown System (FSS)
2. Second Shutdown System (SSS)
3. Chimney Water Injection System (CWIS)
4. Confinement Ventilation System (CVS)
5. First Shutdown System with Electrical Outage (FSSEO)
6. Core Cooling by Forced Convection (FCCC)
7. Core Cooling by Natural Convection (NCCC)
8. Siphon Effect Breaker System (SEB).

In this work, the effect of redundancy allocation on the safety performance of the first five systems will be considered. Main features of these systems are described as follows.

First Shutdown System (FSS)

The FSS is responsible for the fast shutdown of the reactor (terminates rapidly the neutron chain reaction) whenever safety limits are exceeded.

The control mechanisms associated with each of the six absorbing rods are identical. Each mechanism is provided with its own independent compressed air tank, two redundant trigger valves, hose, pneumatic cylinder, magnetic coupling and stepping electrical motor with its corresponding gear box.

The shutdown will be achieved by the injection of six neutron absorbing rods into the reactor core. At least any five of the rods have to be inserted to shutdown the reactor. The fast shutdown will be carried out by means of a compressed air injection from an airtank (diving tank) to the cylinder-piston mechanism through a flexible hose. It will be started by an opening signal applied to two redundant solenoid valves [10].

The safety action of absorbing rods is dependent upon the force of gravity aided by compressed air and it is initiated automatically by the reactor protection system or manually by the operators.

Second Shutdown System (SSS)

The SSS is responsible for reactor shutdown if the FSS fails. It is made up of four trains which will inject a gadolinium nitrate solution into four chambers, one placed on each wall of the chimney that surrounds the core. Each of the four trains basically consists of a tank with the gadolinium solution normally pressurized with N_2, two redundant injection valves, piping and an injection chamber.

A depressurization tank, common to the four systems is provided with two redundant 3-way depressurization valve. The system has four trains and the successful performance of at least any three of them will be sufficient to provide the reactor shutdown (3 out of 4 success criteria). Whenever the SSS action is required, the trigger signal will simultaneously open a poison injection valve and vent valves, thus allowing the gadolinium solution to fill the chambers under the driving pressure difference [8].

Chimney Water Injection System (CWIS)

The CWIS is responsible for the injection of water to the reactor chimney in order to maintain the core covered with water in case of an eventual drop of the reactor pool water below the chimney upper edge. This system is triggered by a signal of low water level in the pool. The system has been designed to maintain the chimney filled with water during at least twenty-four hours, thus compensating losses due to residual decay heat (after the reactor shutdown). The system consists of four identical non-redundant tanks (each holds 25% of the required water) and their discharge lines. The lines from the four tanks are combined into a common line that passes through an orifice plate. The flow finally passes through two redundant solenoid operated valves that are used to trigger the system [7].

Confinement Ventilation System (CVS)

The reactor building is provided with CVS, which, in addition to providing comfortable working conditions for reactor personnel, will be capable of confining accidental leaks.

The CVS is composed of two modules: the containment system and the radioactive product removal system. The first system function is to isolate the external environment from radioactive contaminants that could eventually be liberated during an accidental situation. The functions of the second system are to reduce doses incurred by the facility personnel in case of contamination of the reactor building air and to control the atmospheric release so that the limits set by the regulatory body are not exceeded [9].

Methodology

In order to study the effect of redundancy allocation on the safety performance of the ETRR-2 safety systems and on the reactor overall safety level, the methodology presented here was adopted.

Fault tree analysis was used in the evaluation of the failure probabilities (probability of the top event) of the ETRR-2 safety and safety related systems. These failure probabilities were evaluated for three different cases. These cases are as follows: case #1, which considers removal of the redundant components from the existing safety system; case #2, which represents the existing safety system, and case #3, which considers adding redundant components to the existing safety system [2].

Figure 2 through Fig. 5 present the fault trees for FSS, FSSEO, SSS, CWIS, and CVS, considering the three cases mentioned above.

For the FSS, case #1 includes removal of a redundant solenoid valve, while case #3 includes the addition of a redundant solenoid valve and a redundant hose pipe, as shown in Fig. 2.

For the SSS, case #1 includes removal of a solenoid valve in the train path, removal of a redundant 3-way valve in the venting path, and keeping only one pressure sensor in the low pressure detection path. However, case #3 includes the addition of a redundant venting valve, a redundant solenoid valve in the train path, and a redundant pressure sensor in low pressure detection path, as shown in Fig. 3.

For the CWIS, case #1 includes the removal of a redundant solenoid valve and the removal of a level sensor in the level sensors path, while case #3 includes the addition of a redundant solenoid valve and a level sensor in the same path, as shown in Fig. 4.

For the CVS, and due to the fact that no redundant components are installed in the already existing system, only the failure probability of the system has been evaluated considering case #2 and case #3. The latter includes the addition of redundant two different dampers

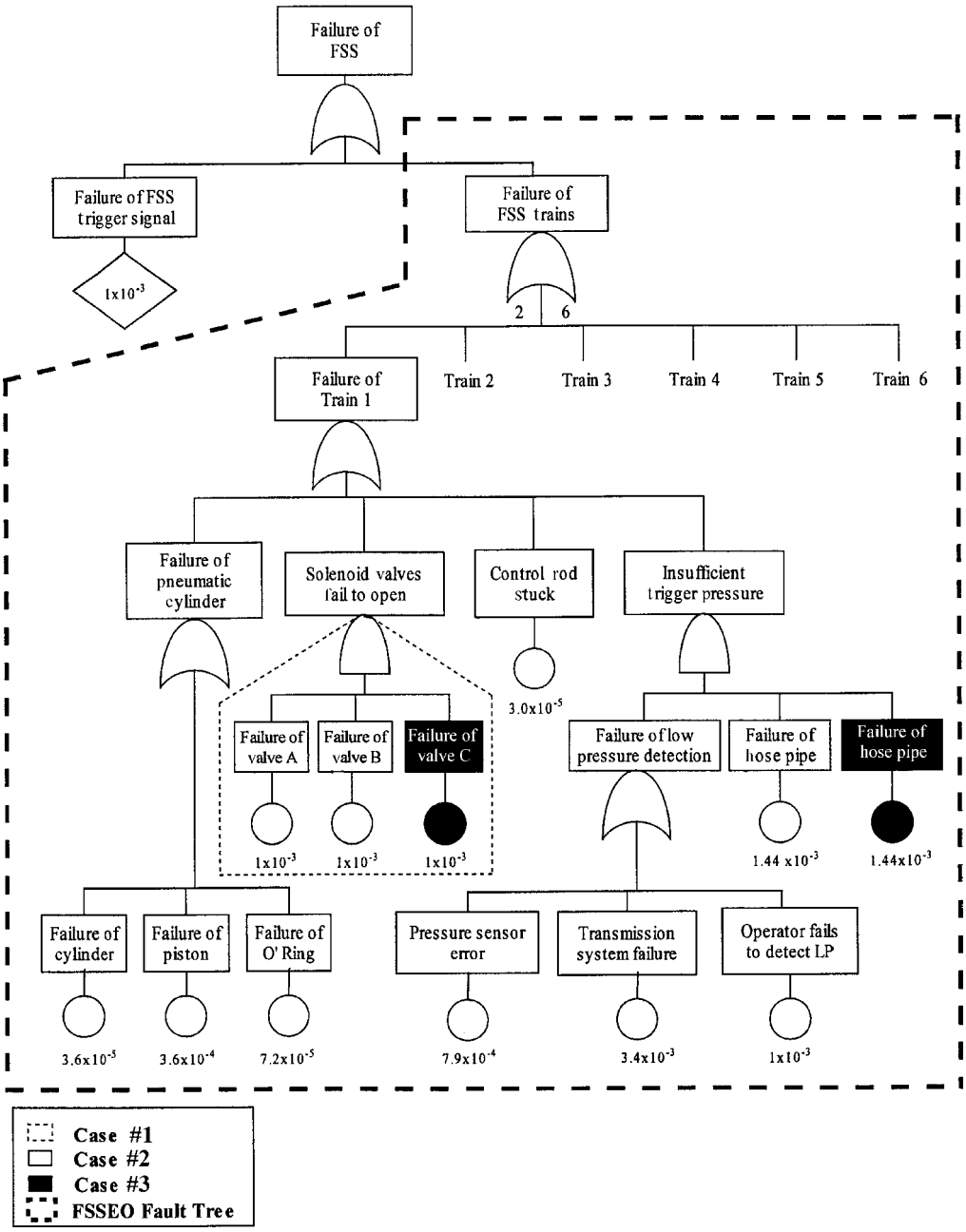

Fig. 2. Fault tree of the First Shutdown System.

and a redundant airtight valve to the already existing system, as shown in Fig. 5.

Once the failure probabilities for the safety systems are determined, they are introduced as headings to the event trees for the analysis of initiating event. The annual occurrence probability of each sequence path is, then, calculated considering the three following cases: #1, #2 and #3, mentioned above.

Failure rates of the components involved in the fault trees are extracted from ETRR-2 Safety Analysis Report [10].

For the purpose of demonstration of the effect of the redundancy allocation on the annual probability occurrence of the initiating events, two initiating events from the postulated events in the ETRR-2 safety analysis have been considered in this study. These initiating events are the loss of the heat sink and the loss of primary system coolant.

The event trees

Event trees for the Loss of Heat Sink and Primary System Coolant initiating events are presented in Figs. 6 and 7, respectively. The annual occurrence probabilities of each sequence path of these initiating events were calculated [2] and presented in the same figures for the three considered cases, case #1, case #2 and case #3.

Figure 6 shows that the annual occurrence probability for the sequence path ABcE has been decreased from 8.664×10^{-7} (case #2) to 2.0732×10^{-7} (case #3),

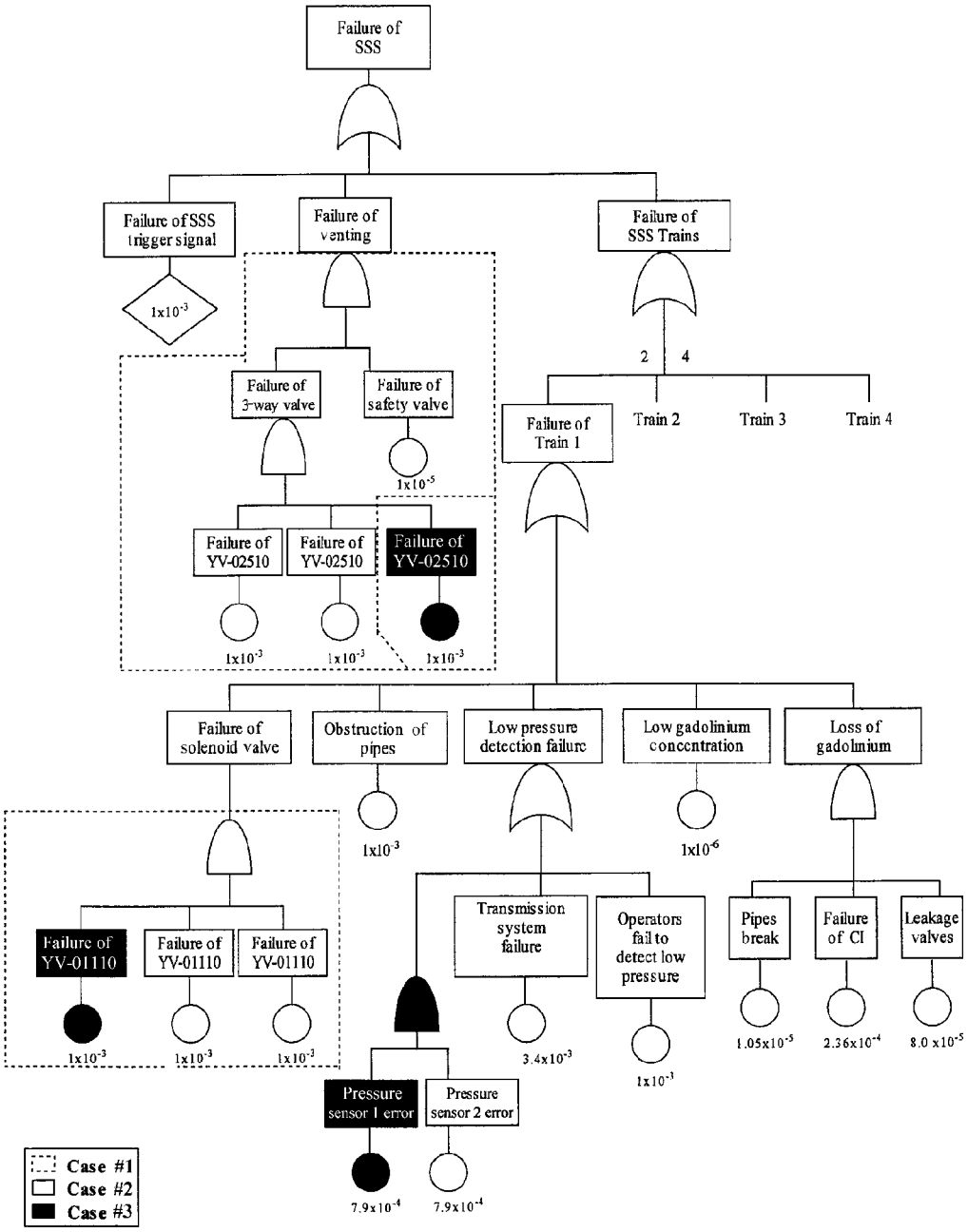

Fig. 3. Fault tree of the Second Shutdown System.

representing decrease of 76% in the annual probability. Sequence path ABcE represents a Plant Status (PS) of severe accident with 80% core damage, core covered with water, and failure in CVS (SAC). The annual occurrence probability of the sequence path ABcE has decreased by the same previous value. This path also represents SAC status. This decrease in the annual occurrence probability is due to the improvement of the failure probability of the CVS by allocating redundant components.

Figure 6 shows also that a slight decrease in annual occurrence probability is achieved for the paths that involve the RSS (Reactor Shutdown System function, which includes FSS and SSS). This is mainly because a slight decrease in the failure probability has been achieved with the allocation of redundant components to the FSS and SSS, as discussed above. For example, the annual occurrence probability of the sequence path ABcE has decreased from 8.673×10^{-7} (case #1) to 8.664×10^{-7} (case #2).

Figure 7 shows also that the annual occurrence probability has been decreased for the sequence paths that involve the CVS and CWIS. This decrease in the annual probability has been achieved due to the redundant component allocations, as discussed above.

The decrease in the annual probabilities is observed in the paths AbcDE, AbCdE, AbCDE, ABcE, and ABCE, which result in Plant Status of conditions AW, H, SAU, SAC, and SAU, respectively. This decrease, due to improvement of the reliability of the CVS for the primary system coolant accident, was found to be 76% and 16% for the CWIS. In Fig. 7, the PS, H repre-

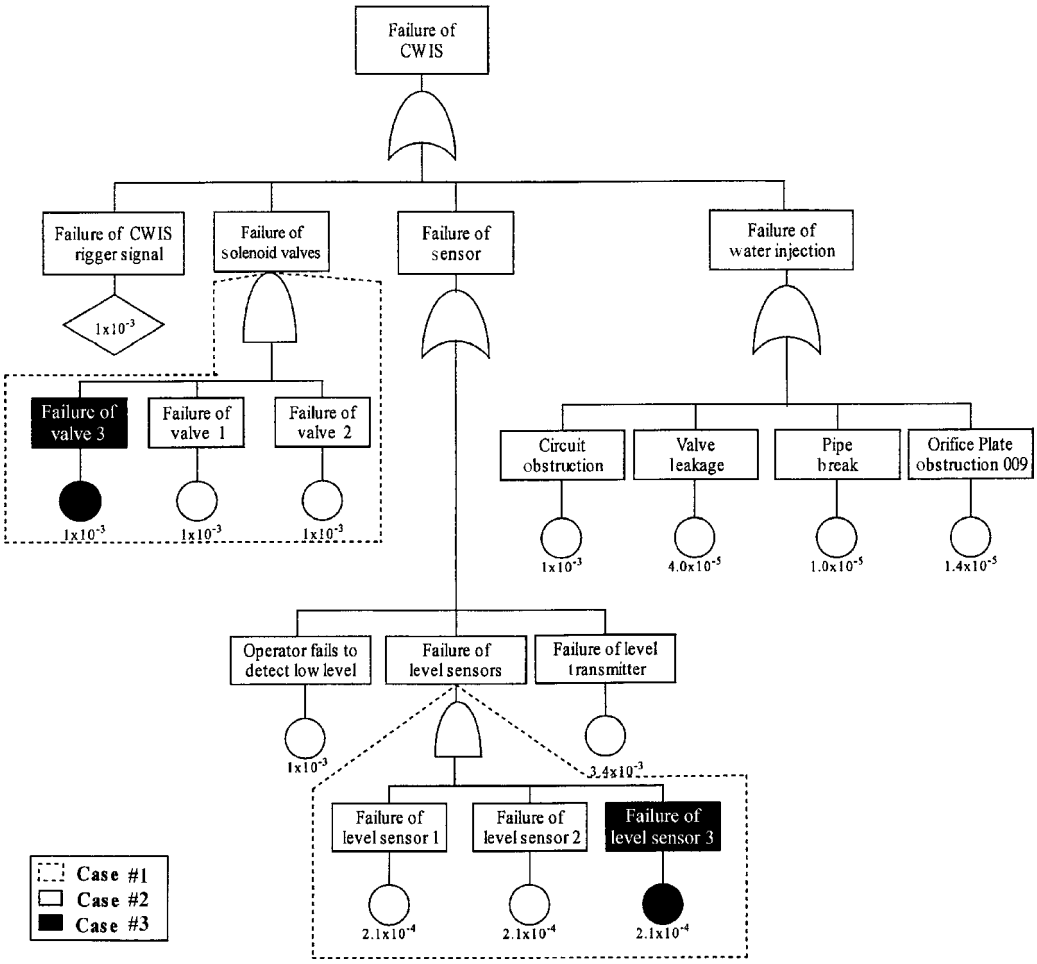

Fig. 4. Fault tree of the Chimney Water Injection System.

sents high damage to the reactor core (50%), SAU represents severe damage to the reactor core (80%) with core uncovered with water and failure of the CVS.

Results and discussions

The fault trees for the safety systems of ETRR-2 have been evaluated and the failure probabilities of these systems were calculated for the three cases presented above [2]. The results are summarized in Table 1. This table shows that, for all safety systems, the failure probability generally decreases with increasing number of redundant components. This table shows that considerable decreases in the failure probability of the SSS and CWIS are obtained with increasing redundant components. Due to redundant component allocation, the failure probabilities of the SSS and CWIS have been decreased by 87.78 and 18.6%, respectively. A very high decrease in the failure probability has been achieved by redundancy allocation to the FSSEO. Failure probability has decreased to 1.25×10^{-2} of the previous value.

The calculated failure probabilities reflect the proper design of the already existing safety systems of the ETRR-2. However, Table 1 also shows that further improvement could be introduced to the already existing CVS in order to increase the system reliability. The failure probability of the already existing CVS has been decreased 3 times with redundancy allocation of two dampers and an air tight valve. Decreases in the failure probability of the SSS and FSSEO by 4.59 and 3.41%, respectively, have been achieved due to allocation of some redundant components to the already existing systems.

It is worth mentioning here that for the PSA, all initiating events postulated by the design are analyzed like in the previous section, the path sequences that result in same the plant status are grouped and the total occurrence probability is then calculated. The dose

Table 1. Failure probability of the ETRR-2 safety systems for the considered three cases

System	Failure probability		
	case #1	case #2	case #3
FSS	0.0010338	0.0010038	0.0010037
SSS	0.00230414	0.001227	0.0011731
RSS	0.00100238	0.0010012	0.0010012
CWIS	0.00765239	0.0064514	0.0064504
CVS	0.02058399	0.020584	0.004962
FSSEO	0.000338347	3.842E-06	3.715E-06

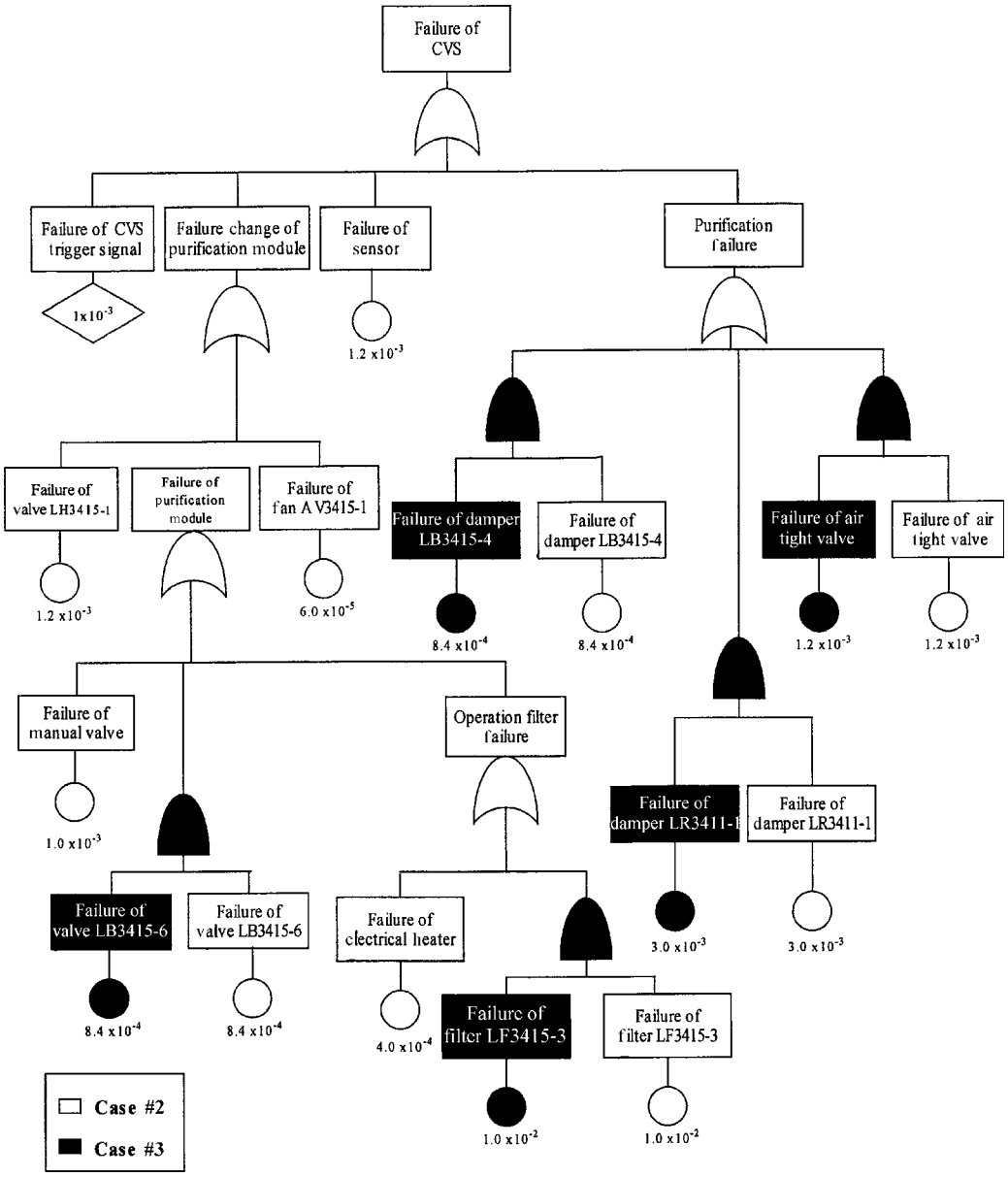

Fig. 5. Fault tree of the Confinement Ventilation System.

consequences to the public and operators are determined for every plant status.

02 (A)	RSS (B)	PPS (C)	NCCC (D)	CVS (E)	Sequence Path	Annual Occurrence case #1	case #2	case #3	PS
					1. Abcd	0. 04199669	0. 04199673	0. 041996736	
					2. AbcD	1.758 E-07	1. 758 E-07	1. 75804 E-07	
					3. AbC	0. 02713377	0. 02713381	0. 027133807	
					4. ABce	4. 1272 E-05	4. 1224 E-05	4. 18796 E-05	SACV
					5. ABcE	8. 6739 E-07	8. 664 E-07	2. 07329 E-07	SAC
					6. ABCe	2. 6665 E-05	2. 6635 E-05	2. 7058 E-05	SACV
					7. ABCE	5. 6041 E-07	5. 5977E-07	1. 33953E-07	SAC
(A) 02	(B) RSS	(C) PPS	(D) NCCC	(E) CVS	Sequence Path	case #1	case#2	case #3	PS
						Annual Occurrence			

Fig. 6. Event tree for Loss of Heat Sink Accident.

03 (A)	RSS (B)	FVSEB (C)	CWIS (D)	CVS (E)	Sequence Path	Annual Occurrence case #1	case #2	case #3	PS
					1. Abcde	0. 008478403	0. 008488673	0. 00862408	AWV
					2. AbcdE	0. 000178187	0. 000178403	4. 26943 E-05	AW
					3. AbcDe	6. 53803 E-05	5. 51198 E-05	5. 599 E-05	AWV
					4. AbcDE	1. 37407 E-06	1. 15843 E-06	2. 77184 E-07	AW
					5. AbCde	1. 73824 E-05	1. 74034 E-05	1. 7681 E-05	HV
					6. AbCdE	3. 65318 E-07	3. 65761 E-07	8. 75316E-08	H
					7. AbCDe	1. 34042 E-07	1. 13006 E-07	1. 1479 E-07	SAUV
					8. AbCDE	2. 81712 E-09	2. 37501E-09	5. 68281 E-10	SAU
					9. ABce	8. 57271 E-06	8. 56288E-06	8. 69899 E-06	SACV
					10. ABcE	1. 80169 E-07	1. 79963 E-07	4. 30652 E-08	SAC
					11. ABCe	1. 75757 E-08	1. 75556 E-08	1. 78346 E-08	SAUV
					12. ABCE	3. 69382 E-10	3. 68958 E-10	8. 8292 E-11	SAU
(A) 03	(B) RSS	(C) FVSEB	(D) CWIS	(E) CVS	Sequence Path	case #1	case #2	case #3	PS
						Annual Occurrence			

Fig. 7. Event tree for the Primary System Coolant Accident.

Conclusions

The evaluation of the fault trees for the ETRR-2 reactor using redundancy allocation technique has been carried out. The analysis shows that the safety systems failure rates are generally decreased with allocation of redundant components. The already existing safety systems are considerably reliable. The failure rates for the safety systems have been analyzed considering allocation of more redundant components. In the case of SSS and CWIS there is a slight improvement to the reliability. But the analysis has shown that further improvements could be introduced to the CVS. The failure rate of the CVS has been shown to be significantly decreased by allocating two dampers and an airtight valve to the line of the emergency mode of the system.

The probabilistic safety assessment of the two selected initiating events has shown that the allocation of these redundant components to the already existing systems will reduce the annual occurrence probability of the severe and high core damage accidental conditions. This decrease in the occurrence probability is 76% and 16% for the CVS and CWIS, respectively.

References

1. Abdelrazek ID (2002) The development of the MPR project. In: Proc of the 5th Arab Conf in the Peaceful Uses of Atomic Energy, November 2000, Lebanon, I:41–66
2. Elsayed AE (1996) Reliability engineering. Addison Wesley Longman, USA
3. IAEA (1987) Probabilistic safety assessment for research reactors. IAEA-TECDOC-400. IAEA, Vienna
4. IAEA (1989) Applications of probabilistic safety assessment to research reactors. IAEA-TECDOC-517. IAEA, Vienna
5. IAEA (1992) Application of the single failure criteria. IAEA Safety Series 50-P-1. IAEA, Vienna
6. IAEA (1994) Safety assessment of research reactors and preparation of the safety analysis report. Safety Series 35-G-1. IAEA, Vienna
7. INVAP-AEA (1995) CWIS descriptive technical report. ETRR-2 Document #0767-0240-2VAPE-003-1B
8. INVAP-AEA (1995) Second shutdown system descriptive technical report. ETRR-2 Document #0767-0850-2VAPE-003-1A
9. INVAP-AEA (1996) Reactor hall ventilation system: Technical report. ETRR-2 Document #0767-3410-2VAPQ-001-1O
10. INVAP-AEA (1999) Final safety analysis report of ETRR-2. Document #0767-5325-3IBLI-001-1A