Available online at www.sciencedirect.com
SCIENCE DIRECT®
Annals of Nuclear Energy 32 (2005) 63–87
annals of NUCLEAR ENERGY
www.elsevier.com/locate/anucene

Reliability analysis of shutdown system

C. Senthil Kumar [a,*], A. John Arul [b], Om Pal Singh [c], K. Suryaprakasa Rao [d]

[a] *Aerb-Safety Research Institute, IGCAR Campus, Kalpakkam 603102, India*
[b] *Indira Gandhi Centre For Atomic Research, Kalpakkam 603102, India*
[c] *Atomic Energy Regulatory Board, Niyamak Bhavan, Anushaktinagar, Mumbai 400094, India*
[d] *Industrial Engineering Division, Anna University, Chennai 60025, India*

Received 7 May 2004; accepted 2 August 2004
Available online 11 September 2004

Abstract

This paper presents the results of reliability analysis of Shutdown System (SDS) of Indian Prototype Fast Breeder Reactor. Reliability analysis carried out using Fault Tree Analysis predicts a value of 3.5×10^{-8}/de for failure of shutdown function in case of global faults and 4.4×10^{-8}/de for local faults. Based on 20 de/y, the frequency of shutdown function failure is 0.7×10^{-6}/ry, which meets the reliability target, set by the Indian Atomic Energy Regulatory Board. The reliability is limited by Common Cause Failure (CCF) of actuation part of SDS and to a lesser extent CCF of electronic components. The failure frequency of individual systems is $<1 \times 10^{-3}$/ry, which also meets the safety criteria. Uncertainty analysis indicates a maximum error factor of *5* for the top event unavailability.

1. Introduction and scope

The purpose of Shutdown System (SDS) (IGCAR, 1997) in a nuclear reactor is to promptly terminate the fission chain reaction and thereby ensure safety during

* Corresponding author. Tel.: 91 4114 280164.
E-mail address: cskumar@igcar.ernet.in (C.S. Kumar).

0306-4549/$ - see front matter © 2004 Elsevier Ltd. All rights reserved.
doi:10.1016/j.anucene.2004.08.002

Nomenclature

AERB	Atomic Energy Regulatory Board
AS	Actuation System
CCF	Common Cause Failure
CSR	Control and Safety Rods
CSRDM	Control Safety Rods Drive Mechanism
DBE	Design Basis Event
DND	Delayed Neutron Detector
DSL	Design Safety Limit
DSR	Diverse Safety Rods
DSRDM	Diverse Safety Rods Drive Mechanism
EMC	Electro Magnetic Compatiblity
EF	Error Factor
FBTR	Fast Breeder Test Reactor
FIT	Fine Impulse Test
HEP	Human Error Probability
PCSL	Pulse Coded Safety Logic
PFBR	Prototype Fast Breeder Reactor
PLD	Programmable Logic Devices
RPS	Reactor Protection System
SA	Sub Assembly
SDS	Shutdown System
SLFIT	Solid State Logic with Fine Impulse Test
TOP	Transient Over Power
TUC	Transient Under Cooling

the Design Basis Events (DBE). Reliability requirements for such important safety critical system are typically in the range of $1E-6$ per reactor year (ry). To achieve such optimistic reliability goals, a reactor shutdown system is designed to tolerate faults and perform its function satisfactorily for a given mission time. Moreover, SDS is required to function during critical and emergency conditions to ensure safety of the nuclear plant. This paper presents the reliability analysis of SDS of Indian Prototype Fast Breeder Reactor (PFBR).

PFBR is a 500 MWe sodium cooled, pool type Fast Breeder Reactor and is in the construction stage at Kalpakkam, INDIA. The scope of this paper is to estimate the reliability of SDS overall design. Fault Tree analysis is used to arrive at the probability of failure of SDS on demand. 'RISK SPECTRUM' software is used for qualitative and quantitative analysis of the Fault Tree. The risk importance analysis, sensitivity analysis and uncertainty analysis are also performed and the results are reported.

2. System description and function

PFBR has two shutdown systems; SDS1 and SDS2. Each shutdown system consists of a Reactor Protection System (RPS), Actuation System (AS) and safety support systems. RPS consists of instrumentation, i.e., sensors to monitor plant parameters, analogue signal processing circuits, SCRAM logic, SCRAM switches (power gates) and power supply. AS consists of Absorber Rods (AR), electromagnets and drive mechanisms to drop or drive the absorber rods into the core. The overall structure is similar for both the SDS as shown in Fig. 1. SDS1 and SDS2 are independent and diverse except for Delayed Neutron Detection (DND) and reactor inlet temperature (θ_{RI}) signals, which are common to both the systems. The two SDS are optically linked (Fig. 1) to improve the reliability of the SDS. Optical inter-link enables both sets of SCRAM parameters, i.e., from RPS1 and RPS2 to trigger both the actuation systems while maintaining electrical isolation.

2.1. Sensors

The plant monitoring is done by functionally diverse set of sensors.

2.1.1. Neutron flux sensors

The neutronic instrumentation consists of 5 fission chambers resistant to radiation and high temperature and having a sensitivity of 1 cps/nv (in pulse mode). Out of these, three sensors are used for safety and two are used for control. These are located in the control plug below lattice plate and about 100 mm above the sub assembly top level during normal operating condition of the reactor. The length of the sensor is 400 mm and diameter is about 50 mm. The flux level (U^{235} thermal eqvt. flux) at the middle level of the sensor varies from 1 nv at shutdown to 1.55×10^9 nv at nominal power of 1250 MW. For safety, neutronic channels in 2/3 voting mode monitor the neutronic flux, ϕ. SCRAM takes place on power (P) and the derived parameters like reactor period (τ) and reactivity (ρ) when their thresholds are crossed. These parameters provide protection against transient over power, transient under-cooling and anomalous reactivity events.

2.1.2. Thermocouples

Four fast response thermocouples mounted on the central canal plug monitor the central fuel sub assembly (SA) sodium outlet temperature (θ_{CSAM}) and used on a 2/3 voting mode with one back up. Four thermocouples within thermo-well are provided in each of the two primary sodium pump suction side to monitor the reactor inlet temperature (θ_{RI}). θ_{RI} and θ_{CSAM} thermocouple signals are processed through triplicated hardwired electronic circuits. Two thermocouples each (within a single thermo-well) are provided over the other fuel subassemblies with 2/2 voting mode, to monitor individual SA sodium outlet temperature (θ_i). On-line computed parameters like the mean fuel SA sodium outlet temperature (θ_M) and mean core sodium temperature rise ($\Delta\theta_M$) are obtained as follows:

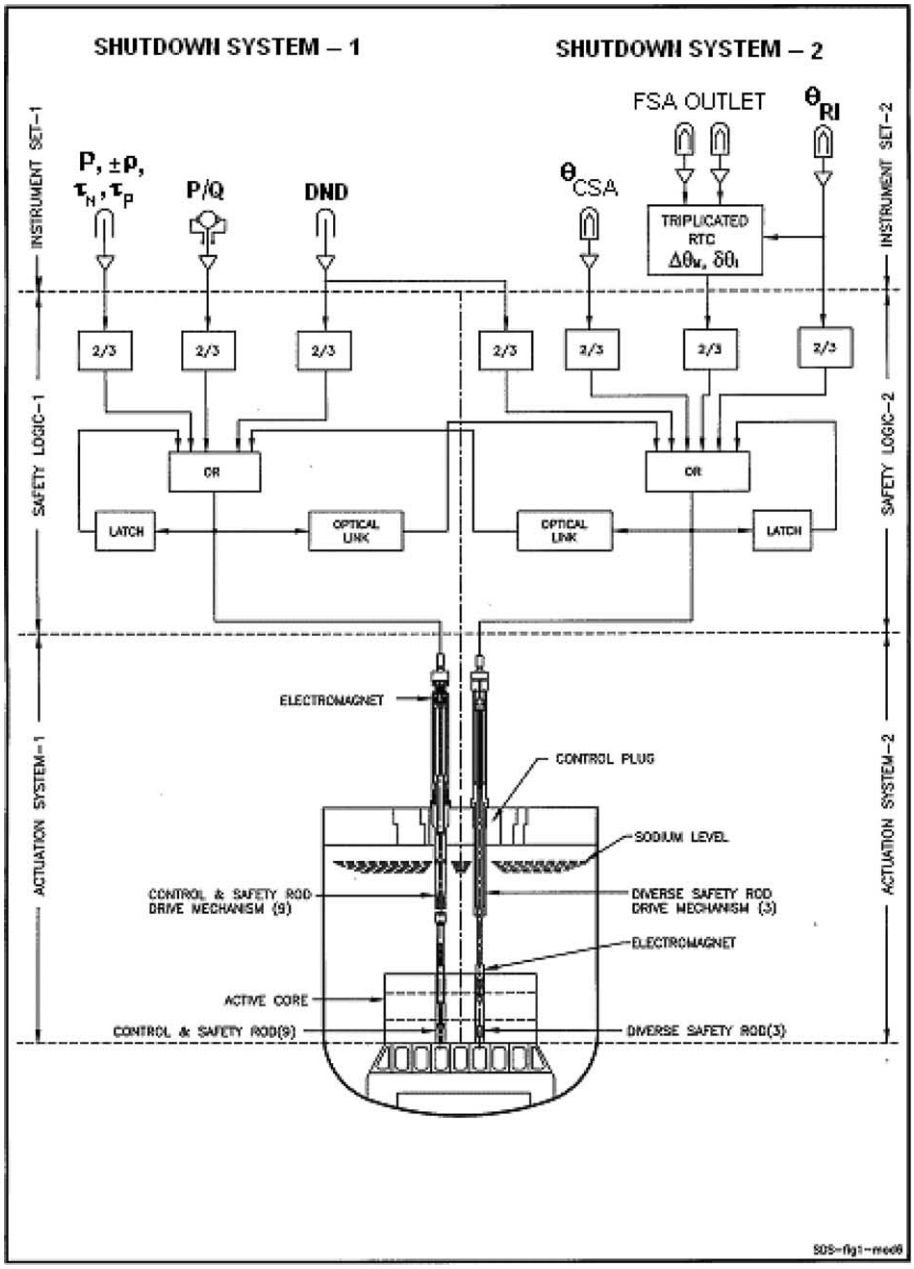


Fig. 1. Shutdown systems.

$$\theta_M = (1/N)\Sigma\ \theta_i, \quad \Delta\theta_M = \theta_M - \theta_{RI},$$

where N is the number of SA. The deviation ($\delta\theta_i$) of individual SA sodium outlet temperature (θ_i) from the expected value (θ_e) is obtained as

$$\delta\theta_{\mathrm{i}} = \theta_{\mathrm{i}} - \theta_{\mathrm{e}} = \theta_{\mathrm{i}} - (a_i.\Delta\theta_{\mathrm{M}} + \theta_{\mathrm{RI}}).$$

Here, a_i is the ratio of temperature rise of the ith SA to the mean temperature rise in the core.

θ_{CSAM}, $\Delta\theta_{\mathrm{M}}$, θ_{RI} and $\delta\theta_{\mathrm{i}}$ cause SCRAM when their thresholds are crossed. SCRAM on θ_{CSAM} takes care of Design Safety Limits (DSL) on clad and coolant. SCRAM on $\Delta\theta_{\mathrm{M}}$ takes care of global cooling changes in the core and SCRAM on θ_{RI} takes care of disturbances in secondary and steam water circuits affecting reactor core. SCRAM on $\delta\theta_{\mathrm{i}}$ takes care of local faults in the SA.

Rearranging the expression for $\delta\theta_{\mathrm{i}}$ as $\delta\theta_{\mathrm{i}} = (\theta_{\mathrm{i}} - \theta_{\mathrm{RI}}) - a_i.\ \Delta\theta_{\mathrm{m}}$, it can be seen that $\delta\theta_I$ is the difference between $(\theta_{\mathrm{i}} - \theta_{\mathrm{RI}})$ and a threshold varying with SA radial position and power/flow ratio $(a_i.\Delta\theta_{\mathrm{M}})$. This is required for faster response at power less than 20% nominal. The trip is on a function of $(\theta_{\mathrm{i}} - \theta_{\mathrm{RI}}, \Sigma\theta_{\mathrm{i}})$ instead of on the simple difference $(\theta_{\mathrm{i}} - \theta_{\mathrm{RI}})$. Software is preferred for flexibility. The required computations for θ_{M}, $\Delta\theta_{\mathrm{M}}$ and $\delta\theta_{\mathrm{i}}$ are carried out using computers meant for class I applications, in 2/3 voting mode.

2.1.3. Electromagnetic flow meters

Electromagnetic flow meters (one per pump) measure sodium flow (Q) in primary sodium circuit. Each flow meter consists of three pairs of electrodes. This signal is used to obtain power to flow ratio (P/Q) in 2/3 voting, which is used as another SCRAM parameter to take care of global cooling changes in the core.

2.1.4. Delayed neutron detectors

Delayed neutron detectors (DND) are provided to detect and SCRAM the reactor for fuel clad rupture. Eight identical DND blocks each with three detectors are placed at the inlet of the four IHX. i.e., Two blocks per IHX. The transit time of sodium from any of the failed fuel pin to the nearest detector location is 6–49 s. The DND outputs are connected to both SCRAM logics so that the reactor is brought automatically to a safe shutdown state in case of fuel clad failure. The system provides triplicated detection and uses 2/3 logic to avoid spurious SCRAM. For reliability analysis it is conservatively assumed that each block is required to detect events from a particular region in core.

2.2. Analogue signal processing circuits

Signals from each sensor are processed with suitable analogue signal processing circuits and then fed to comparator. The resulting digital signal is processed by SCRAM logic.

2.3. SCRAM logic

The SDS1 uses conventional Solid State Logic with online Fine Impulse Test (SLFIT). It is built using Programmable Logic Devices (PLD). SLFIT (Fig. 2(a)) consist of safety logic core, output stage and annunciation. FIT logic is designed to check unsafe and safe faults of SLFIT apart from the self-diagnostic tests. Safety logic in SDS2 employs Pulse Coded Safety Logic (PCSL) technology, where the logic state 1 is encoded as a sequence of pulses rather than a high voltage level. In PCSL, the presence of pulse train at the logic output stage, keeps the electromagnet energized and if logic is stuck up at 0 or 1 anywhere in the chain, it results in trip state of the chain This technique is self-diagnostic and hence there is no need for separate online testing (Fig. 2(b)).

2.4. SCRAM switch

The outputs from 2/3 voting logic are combined using OR gates in the case of SDS1 and Guard Line Logic in the case of SDS2 and fed to SCRAM switches (power gates). The SCRAM switches are pairs of transistors in series with electromagnet coils to de-energise the electromagnets on a SCRAM signal (Fig. 2(c)).

2.5. Actuation system

Two types of mechanisms and absorber rods are provided (Babu et al., 1997; Vijayashree et al., 1997. Absorber Rods (AR) of system 1 are called Control and Safety Rods (CSR) and the AR of system 2 are called Diverse Safety Rods (DSR). There are 9 CSR and 3 DSR. Clearance between stationary sheath and mobile absorber rod is higher in DSR compared to that in CSR. The drive mechanisms of CSR and DSR are termed, respectively, as CSRDM and DSRDM. During normal operation, the DSR s will be in fully raised position and all CSRs will be in a banked position (all rods at same level) so as to achieve criticality and power operation.

When a SCRAM signal is given, the mobile assembly of CSRDM along with CSR is released from the electromagnet and falls under gravity. However, in the case of DSR and DSRDM, only DSR is released from the electromagnet and falls under gravity.

Three phase induction motors are provided to drive the mechanisms. The operation of CSRDM is through control console whereas that of DSRDM is from the control panel. Control logic ensures that only one CSR or DSR can be selected at a time and CSR are raised only after all the DSR are fully raised. The EM coils of the two systems are connected to two independent safety logics and separate cable routings to reduce the probability of common cause failures. An optical link is provided to actuate a system when the other system gets actuated.

The reactor control is fully manual. Power raising, setback and regulation is done manually by adjusting CSR positions from the control console. The CSR positions are always balanced. The DSR are kept fully out during operation, and used only for shutting down the reactor.

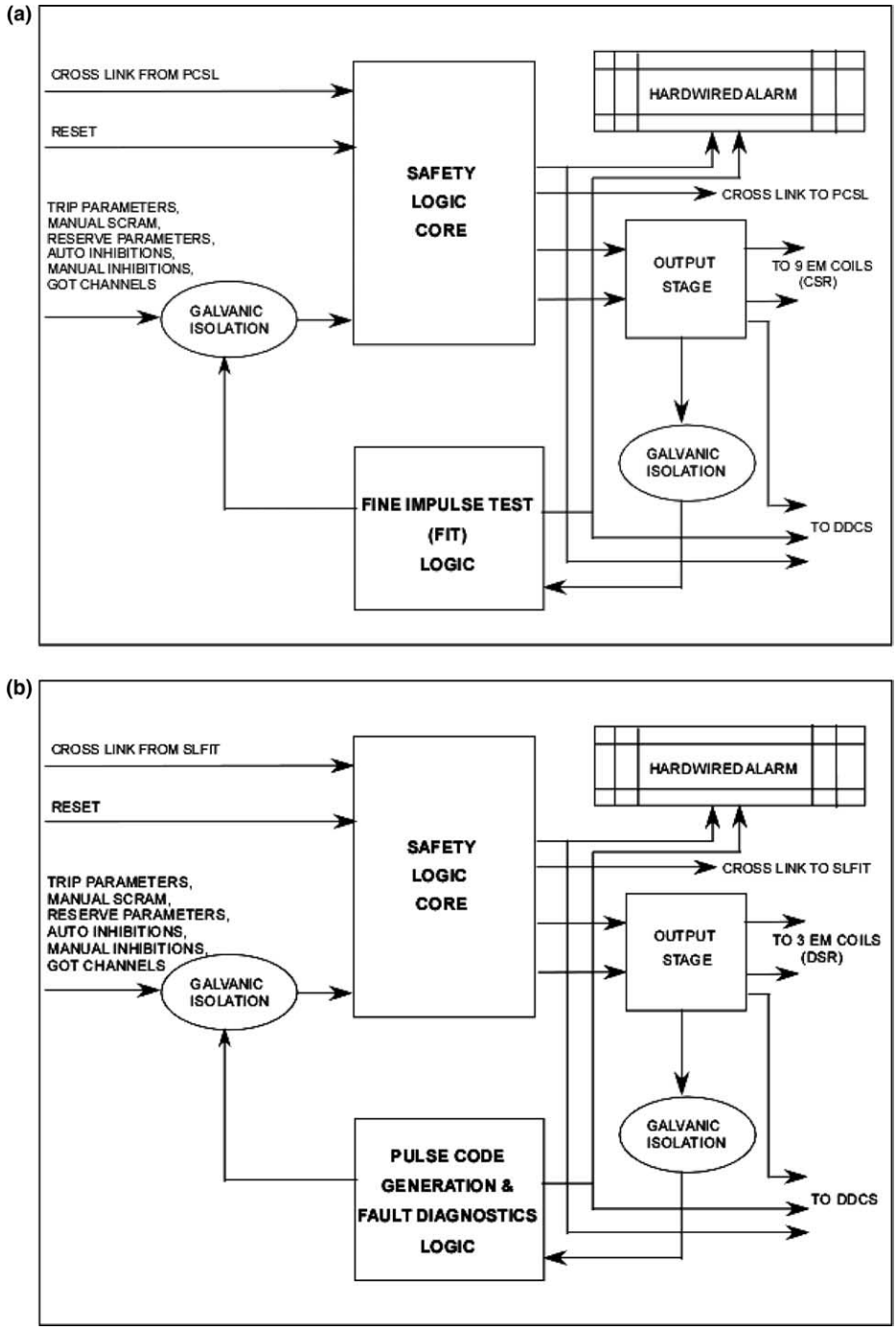


Fig. 2. (a) Block diagram of safety logic with FIT (SLFIT), (b) block diagram of pulse coded safety logic (PCSL) (c) scram switches of SDS1 and SDS2.

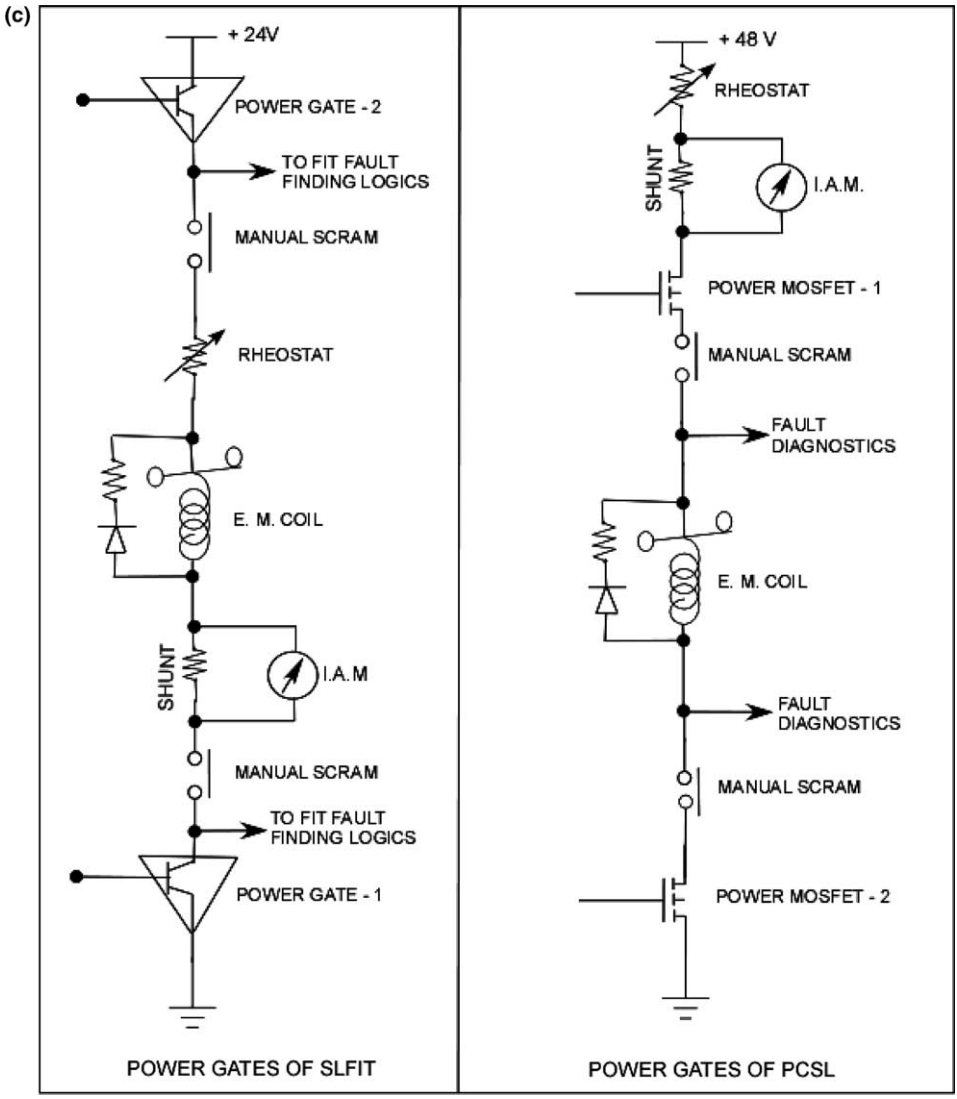


Fig. 2 (*continued*)

2.6. Design basis events and SCRAM parameters

The SCRAM parameters have been identified based on the analysis of DBE having potential to increase fuel, clad and coolant temperatures beyond their DSL. This may occur because of two reasons, i.e., either due to Transient Over Power (TOP) or due to Transient Under Cooling (TUC). In TOP, power production is more than the nominal heat removal capability, which affects the fuel temperature immediately whereas in TUC, power production continues at the nominal level but heat removal

Table 1
DSL for coolant, clad and fuel temperatures

Event category	Hot spot temperature limits		
	Coolant (K)	Clad (K)	Fuel (K)
1	–	973	<Melting point
2	<Boiling	1073	<Melting point
3	<Boiling	1173	<Melting point
4	<Boiling	1473	$\leq$50% (Melting area in max rated pellet)

Table 2
List of reactor SCRAM parameters

S.No.	Parameter	Threshold	Time constant (s)
1	P	110% Nominal	0.05
2	τ_P	10 s	2.4
3	ρ	±10 pcm	0.05
4	DND	[a]	[a]
5	P/Q	1.10	0.05
6	θ_{CSAM}	Nominal + 10 K	0.3
7	$\Delta\theta_M$	Nominal + 10 K	8
8	$\delta\theta_I$	10K	8
9	θ_{RI}	Nominal + 10 K	8

[a] To be decided later.

capability falls below nominal. A detailed plant dynamics study has been carried out to evaluate the SCRAM parameters for TOP and TUC events (Kasinathan et al., 1996; Kasinathan et al., 1997), The response times of the system is accounted in the analysis. The DSL on the coolant, clad and fuel temperatures (Table 1) for the different categories of the DBE are respected. The list of SCRAM parameters and their thresholds are given in Table 2 and SCRAM parameters identified by carrying out transient analyses of all the DBE, which challenge the DSL, are given in Table 3.

Table 3
DBE that require SCRAM and the available SCRAM parameters

S.No.	DBE	SCRAM parameters	
		SDS1	SDS2
1	TOP during low power and/or start-up	ρ, P/Q	θ_{CSAM}[a]
2	TOP during power operation	P	θ_{CSAM}
3	Off-site power failure	P/Q	θ_{CSAM}
4	Primary pipe rupture	P	θ_{CSAM}
5	One PSP seizure	P/Q	θ_{CSAM}
6	SA faults	ρ (and DND)	$\delta\theta_I$ (and DND)
7	Fault in Secondary Sodium circuit and Water Steam Circuit affecting core	θ_{RI} (and ρ)	θ_{CSAM}

[a] θ_{CSAM} and $\Delta\theta_M$ are available for power >15%. ρ is available for power >5%. PSP = Primary Sodium Pump.

SCRAM is followed by automatic drive down of all the rods to ensure insertion of the rods. Indications in control room are provided to know if the mobile assemblies of drive mechanisms reach the bottom limit. In addition to these parameters provision for manual SCRAM is incorporated in the design.

The distribution of SCRAM parameters to system 1 and system 2 is also indicated in Table 3. The thresholds are set close to the normal operating levels after accounting for: (i) operation margins; (ii) fluctuations in the signal around their mean value; (iii) errors that could occur in setting the thresholds; (iv) inaccuracies of instrumentation.

3. Test procedure

The components starting from the sensors, up to signal processing circuits there are automatic discordance tests and manual tests including dynamic testing of system responses. The comparator and digital logic circuits have automated testing provisions, i.e., FIT for the SLFIT and self test for PCSL.

The CSR & CSRDM and DSR & DSRDM have rod exercising tests and drop tests to ensure compliance with the drop times used in safety analysis.

4. Success criteria

The demand on the shutdown system is said to be successful if at least eight out of the nine CSR or two out of the three DSR are inserted into the core when any parameter crosses its SCRAM threshold. Failure criterion is 2/9 for CSR and 2/3 for DSR. For 12 rods, failure criterion is conservatively 4/12. Manual SCRAM and drive down of the AR is not considered for the success.

The control rod worth decrease due to full core voiding and resultant flux peaking is less than 10% as core height is only ~100 cm. However, large scale voiding is not foreseen in a pool type LMFBR. The rod placements are designed to minimise shadowing effect.

5. Reliability target

The reliability target for shutdown system stipulated by the Indian Atomic Energy Regulatory Board (AERB) for PFBR is such that the failure frequency of each SDS is less than 1E − 3/ry and the overall failure frequency of the two shutdown systems shall be less than 1E − 6/ry'' (AERB, 1990).

6. System boundary

The system considered in this paper is modelled only at block diagram level as shown in Figs. 1–3(a)–(d).

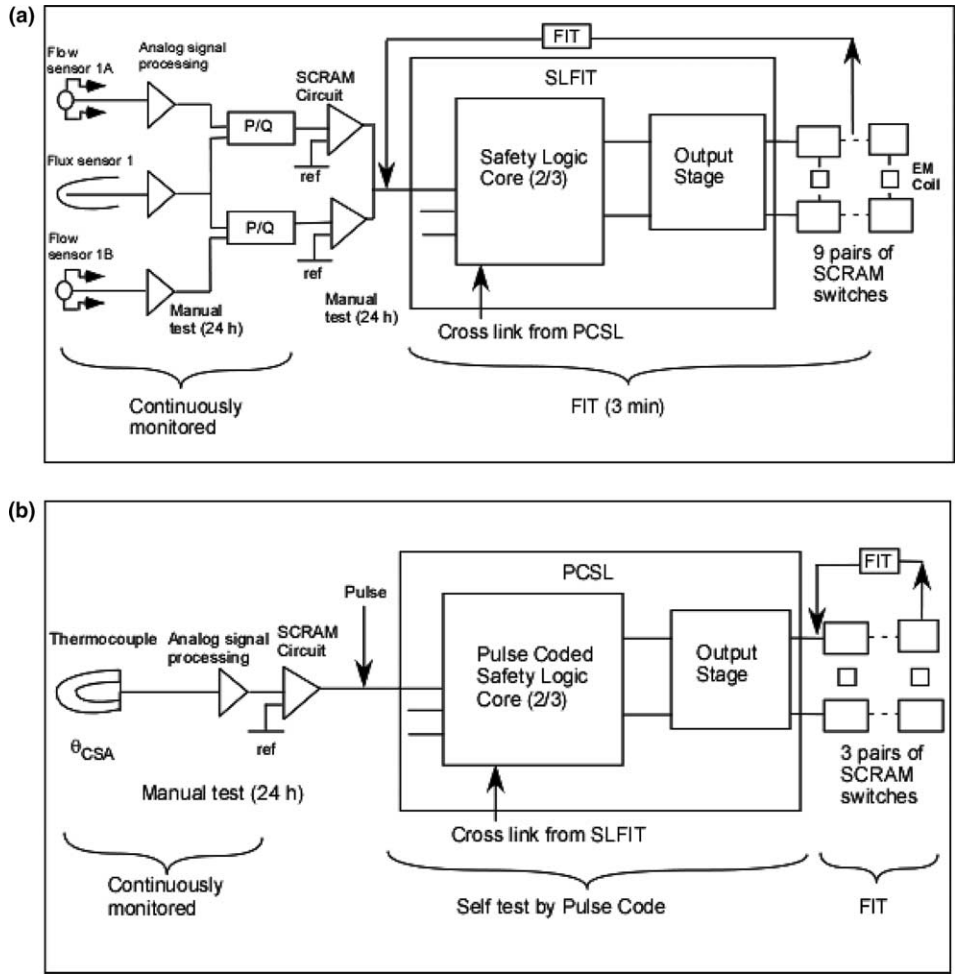


Fig. 3. (a) Simplified logic block diagram of SDS1 for global fault, (b) simplified logic block diagram of SDS2 for global fault, (c) simplified logic block diagram of SDS1 for local fault, (d) simplified logic block diagram of SDS2 for local fault.

7. Assumptions

The following assumptions are made for the purpose of reliability evaluation:

- The cabling, connectors and power supply failure contributions are negligible as design is fail-safe.
- Interfacing systems like start up authorisation, monitoring, etc., does not affect the safety system.
- The SCRAM inhibition logic circuits are not present.

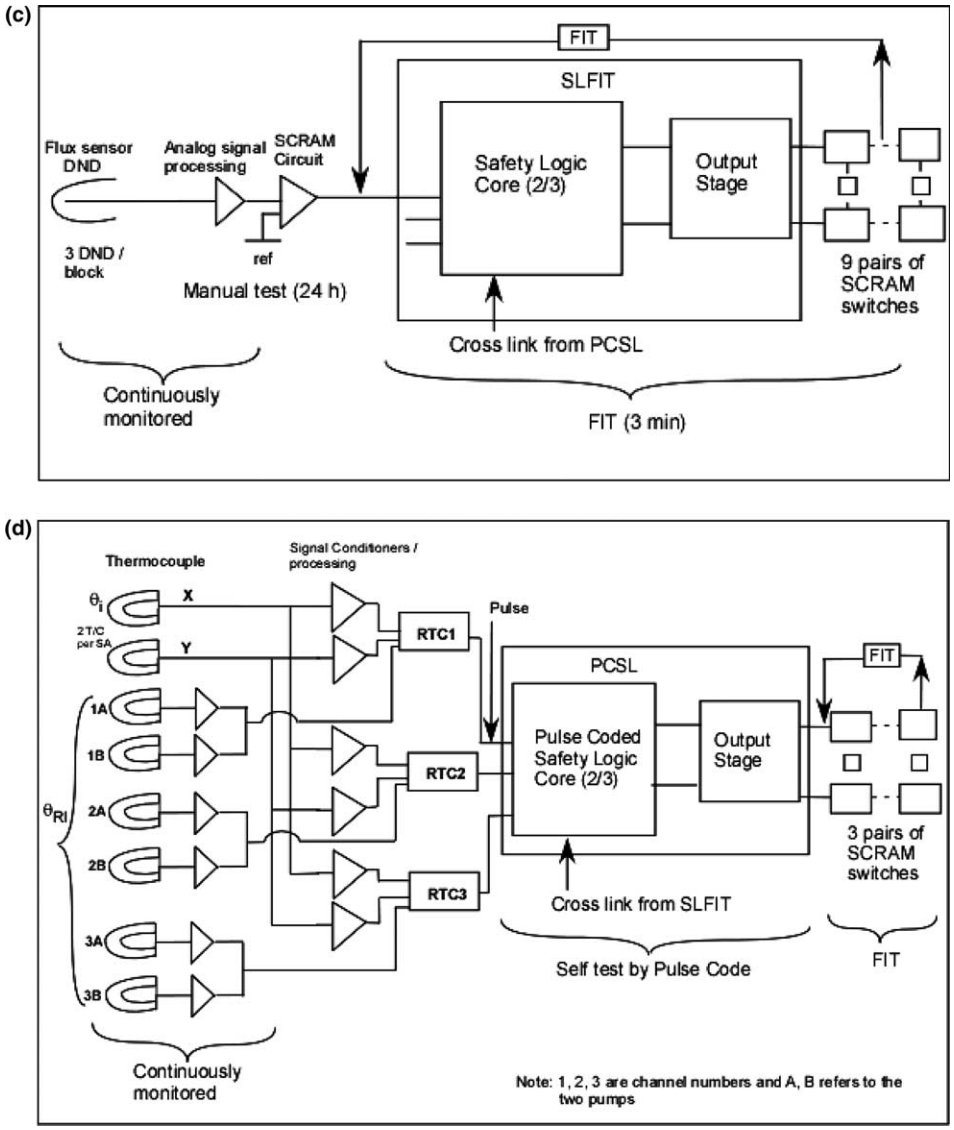


Fig. 3 (*continued*)

- The component/subsystem failure rates are generic values, which are expected to be conservative for the proposed design.
- Low voltage for neutron sensors (HT supply failure) is sensed by Good Operation Trip (GOT) Circuit.
- Fine Impulse Test (FIT) failure does not induce any failure in the system.
- Optical link does not introduce any additional failure modes.

These assumptions are made to enable reliability assessment during the design stage where some of these details are not yet ready.

8. Fault tree description

The reduced model as used for reliability evaluation is shown in Fig. 3(a)–(d). Reliability analysis is carried out, by considering that only neutronic & flow parameters are connected to SDS1 and temperature parameters are connected to SDS2 (except DND and θ_{RI}). Although θ_{RI} is connected to both SDS1 and SDS2, it is conservatively assumed for reliability calculation that it is connected only to SDS2. Optical inter-link enables both sets of SCRAM parameters to trigger the actuation of CSRDM and DSRDM. The presence of optical link necessitates the inclusion of signal from SDS2 in the fault tree for SDS1 and vice versa.

The fault tree for SDS has been constructed using the "immediate cause" approach as recommended by the Indian Atomic Energy Regulatory Board (AERB, 2002). The top event is the failure of SDS to shut down the reactor on demand, i.e., to drop the required number of rods by SCRAM on any parameter crossing the limit. The fault trees for global fault event are given in Appendix A. (The top level Fault Trees are only given and fault trees for similar components are omitted for brevity.) Each stage in the fault tree models the component failure at that stage and the possibility of not getting signal from previous stages.

9. Common cause failure (CCF) analysis

The CCF can be divided into three major groups:

- *Design CCF:* (1) Functional Deficiencies, (2) Design Realization Faults and (3) Engineering Errors.
- *Operation & Maintenance CCF:* (1) Operational Influences including Maintenance and Testing.
- *Environmental CCF:* (1) Environmental Extremes and (2) External Events.

The independence measures considered for the various components/subsystem of SDS are summarised in Table 4. The diversity in the design of the two mechanisms and absorber rods is summarized in Table 5. More gap is provided between DSR and its sheath. More gap between CSR SA leads to increase in bypass flow through the annulus between CSR and its outer sheath and results in reduction in flow through the absorber pin bundle. However, gap provided between CSR and its sheath is adequate such that CSR would operate even during seismic conditions.

There are several CCF models such as β factor model (Edwards and Watson, 1979), Multiple Greek Letter (MGL) model (Kamal and Hill, 1993; Mosleh et al., 1988), shock model and basic parameter model, proposed in literature (Kamal

Table 4
Independence measures between systems in SDS1 and SDS2

Independence measure	Sensors	Analogue signal processing	SCRAM circuit	SCRAM logic	SCRAM switch	Power supply	Cable and connectors
Functional design	X	X		X		–	–
Physical separation	X	X	X	X	X	X	X
Electrical isolation	–	–	–	–	–	X	–
Component technology	X	X	X	X	X	–	–
Design team	X	X	X	X	X	X	–
Manufacturing	–	–	–	–	–	X	–
EMI and EMC	X	X	X	X	X		X
Maintenance and testing	X	X	X	X	X	–	

X: the relevant measures to enhance independence/diversity is present, –: not present, blank : not ascertained/not applicable.

Table 5
Diverse features in CSR, DSR and their drive mechanisms, CSRDM and DSRDM

S.No.	Features	CSRDM/CSR	DSRDM/DSR
1	Designers	Different	Different
2	Magnet temperature	80 °C	500 °C
3	Magnet location	Above core structure	Top of the core
4	Magnet environment	Inter seal argon	Sodium
5	Clearance between the bundle outer sheath and wrapper	Minimum required	More
6	Absorber axial position during operation	Partially in the core	Withdrawn from the core but within wrapper
7	Weight of dropping jiart	~360 kg	~40 Kg
8	Pin wrapper tube	Hexagonal	Circular
9	Part released on SCRAM	Mobile assembly with CSR	DSR only
10	Deceleration	Oil dash pot in air	Sodium dash pot within DSR sheath

and Hill, 1993; Mosleh et al., 1988), We have chosen the β factor method, as it is most suitable for the current level of analysis. In the β factor method, CCF failure rate λ_c is defined as $\lambda_c = \lambda_\tau \beta$, where, λ_τ is the total failure rate and β is a small fraction to account for any implicit dependence between components which cannot be modelled in a fault tree. Based on the redundancy and diversity measures provided, the CCF parameters are chosen (Table 6).

A beta factor of 5% is used for sensors in k/N logic (k failures out of N). As required by β factor model, it is assumed that whenever there is a common cause failure, all N components fail simultaneously. For analogue signal processing circuits of RPS, $\beta = 5\%$ is used. This has been obtained by applying the checklist beta factor method (Humphreys, 1987; Sanjay Alexis, 2000) to the SDS of Fast Breeder Test Reactor (FBTR). No CCF is assumed between signal processing hardware of neutronic channels and temperature measurement channels. No CCF is assumed be-

Table 6
Beta and modifying factors

S. No.	Component	Redundancy/failure criteria	Beta (%)	Modifying factor (Andrews and Moss, 1993)	Comments
1	CSR	2/9: F	10		
2	DSR	2/3: F	10		
3	CSR & DSR	4/12: F	1	0.1	High redundancy and partial diversity
4	Sensors	2/3	5		
5	Signal processing hardware	2/3	5		
6	SCRAM circuit (comparator)	2/3	5		Comparators in SDS1 and SDS2 are diverse
7	SCRAM switch	4	1		
8	SCRAM switches of SDS1 & SDS2	8	1	0.1	High redundancy and partial diversity

Redundancy level of a *k/N:Failure* system is considered as k, as β depends on the number of joint failures required to cause system failure.

tween comparators in system 1 and 2. As PCSL and SLFIT are diverse no CCF is assumed between them. For SCRAM switches, because of their high level of redundancy and simplicity of the component, 1% β is used. A modifying factor of 0.1 is used to multiply β if the minimal cut set term involves both CSR and DSR, to account for the partial diversity. A similar argument holds good for SCRAM switches of SDS1 and SDS2.

9.1. Qualification tests

The components of SDS are safety class −1 (as per IAEA Safety Guide 50-SG-D1 and international practice) and designed for safe shutdown earthquake (IGCAR, 1997). To meet the seismic requirements assembled equipment are subjected to rigorous seismic tests as per site specific seismic spectrum. Equipments such as large panels are qualified by seismic analysis. Other environmental qualification tests including EMC will be carried out as per Indian and IEEE standards (IGCAR, 1997).

10. Human reliability analysis

Human interface comes into picture in two respects for the successful operation of SDS. First, is in the possibility of category-A (Swain and Guttmann, 1983; Ericson, 1990) errors (i.e., is pre-initiator events), during calibration, testing and maintenance operation on SDS and during enabling/disabling trip inhibitions on SCRAM parameters. Second, it is in effecting a manual SCRAM in the event of SCRAM failure. The Human Error Probability (HEP) for the second part is conservatively assumed to be 1.0. Only HEP for pre-initiator tasks, especially, on setting SCRAM threshold

for each of the parameters is considered important and included in the analysis. A Basic Human Error Probability (BHEP) of 0.03 (0.01 – error of commission and 0.02 – error of omission) is assigned to incorrect threshold setting in a channel (Ericson, 1990). The Nominal HEP (NHEP) is obtained as, $(\mathrm{BHEP} \times \mathrm{RF})^{f(n)}$, where RF is Recovery Factor as shown in Table 7 and $f(n)$ is a function of redundancy and dependence as shown in Table 8.

Assuming zero dependence (which is applicable for PFBR, item 4), the Nominal HEP (NHEP) estimated for incorrect threshold setting is $\mathrm{NHEP} = (0.03 \times 0.1 \times 0.01)^2 = \mathbf{(3E-5)^2}$ which is negligible. If high dependence is assumed, NHEP is estimated as $(0.02 \times 0.1 \times .01) \times 0.5^{n-1} = \mathbf{1E-5}$ and if complete dependence is assumed, $\mathrm{NHEP} = (0.02 \times 0.1 \times 0.01) = \mathbf{2E-5}$ (Ericson, 1990, pp. 7–17). For high and complete dependence, error of commission is neglected. Therefore, the human error in threshold setting is conservatively taken as 1E − 5.

11. Failure data

Failure rate data for SDS components have been obtained from international thermal and fast reactor experience and are given in Table 9. In the table, T is the time allowed for operation of reactor with fault in the safety system. FITS: Failure units, 1 in 1E9 (billion) hours and $T' = \max(\tau, T)$.

Table 7
Factors influencing human error probability (Ericson, 1990)

No.	Basic conditions	Conditions applicable for power/temperature channels	RF
1	Compelling signals demanding attention like, annunciation/indication in control room which must be cleared (HEP ~ 1E − 5)	Discordance supervision	–
2	Written verification (0.1)	Required	0.1
3	Post maintenance/calibration tests (0.01)	–	0.01
4	Written daily/shiftly checks (0.1)	Not present	–

Table 8
Factors influencing dependence (Ericson, 1990)

No.	Conditions	Conditions applicable for power/temperature channels	Applicable values/functions
1	Redundancy	Redundancy level of 2 for 2/3 voting	$n = 2$
2	Time reference (2 min)	>2 min between two settings	–
3	Location (visual) reference (4 – feet)	Located in different rooms	–
4	Dependence	Zero dependence based on item 2 and 3	$f(n) = n$

11.1. Modelling reactor outlet thermocouples in fault tree

There are 210 pairs of Thermocouples to measure the SA outlet temperature. Let λ_F be flow blockage frequency per reactor year. The flow blockage frequency per SA, i.e., $\lambda_{SA} = \lambda_F/N$, where $N = 210$ represents the number of subassemblies. The failure frequency of SDS due to LF anywhere in the reactor if the thermocouples will be used in 2/2:S voting is

$$\lambda_{LF} = \mathbf{N}^*\lambda_F/\mathbf{N}^*(2\lambda_t T) + \lambda_f \mathrm{P}(\mathrm{RTC} + \mathrm{SL} + \mathrm{GATES} + \mathrm{ACTSYS}),$$
$$\lambda_{LF} = \lambda_f[(2\lambda_t T) + \mathrm{P}(\mathrm{RTC} + \mathrm{SL} + \mathrm{GATES} + \mathrm{ACTSYS})].$$

The terms within square brackets are evaluated through Fault Tree method.

11.2. Modelling DND in fault tree

There are eight identical DND blocks each with three detectors at the inlet of the IHX to monitor the flux. The system uses 2/3:S logic to avoid spurious SCRAM. The failure frequency per block, i.e., $\lambda_B = \lambda_F/N$, where $N = 8$ represents the number of DND blocks. The failure frequency of SDS due to LF anywhere in the reactor in 2/3:S voting is

$$\lambda_{LF} = \mathbf{N}^*\lambda_F/\mathbf{N}^*(3\lambda_{DND}^2 T^2) + \lambda_F \mathrm{P}(\mathrm{SPC} + \mathrm{SCRCKT} + \mathrm{SL} + \mathrm{GATES} + \mathrm{ACTSYS}),$$
$$\lambda_{LF} = \lambda_F[(3\lambda_{DND}^2 T^2) + \mathrm{P}(\mathrm{SPC} + \mathrm{SCRCKT} + \mathrm{SL} + \mathrm{GATES} + \mathrm{ACTSYS})].$$

The terms within square brackets are evaluated through Fault Tree method.

12. Fault tree analysis

Reliability of SDS is computed by, evaluating the minimal cut sets of the Fault Trees. The software, RISK SPECTRUM has been used for Fault Tree construction, minimal cut-set evaluation, quantification and uncertainty analysis.

The simplified logic block diagrams used for reliability evaluation are shown in Fig. 3a to d. For the purpose of reliability analysis, the DBEs are assigned to, two event groups viz., global and local faults. Global faults represent Transient Under Cooling (TUC) and Transient Over Power (TOP) events. Local faults are events like SA faults. For global fault events, it is assumed conservatively that only P/Q signal is given to SDS1 and temperature signals to SDS2. For local fault event, the signal for SDS1 is DND and the signal for SDS2 is individual SA outlet temperature deviation, $\delta\theta_i$. This being very large in number (i.e., 420 thermocouples in 2/2 voting yielding 210 signals), is processed by RTC. (Refer Section 11 for details on the modelling of reactor outlet thermocouple and DND in fault tree.) The Fault Trees for global fault event are shown in Appendix A. All the DBE are covered by two diverse signals, except for SA total instantaneous blockage, for which only DND signal is available. The basic components in the Fault Tree are represented with an eight-character code. First three characters denote the component category/name, next two characters denote the failure mode and the last three characters denote the component identification number.

Table 9
Basic component/system reliability data

S.No.	Component	Failure mode	Failure rate λ (/h)	Test scheme	Formula (risk spectrum type)	Test/fault persistence/ replacement interval	Reference
1	Neutron detectors	All	7.0E − 6	Continuously monitored	$\lambda T'$ (1)	T = 4 h τ = 24 h (ccf)	IAEA-TECDOC-930 (1997)
2	Thermocouple	All	1.6E − 6	Continuously monitored	$\lambda T'$ (1)	T = 100 h	Bisseau et al. (1982)
3	EM Flow meters	All	4.2E − 6	Continuously monitored	$\lambda T'$ (1)	T = 4 h τ = 24 h (ccf)	IAEA-TECDOC-930 (1997) Bisseau et al. (1982)
4	Processing hardware	All	3.0E − 6	Continuously monitored	$\lambda T'$ (1)	T = 4 h τ = 24 h (ccf)	Assumed
5	SCRAM circuit (comparator)	All	2.0E − 7	Manual test	$\lambda T'$ (1)	T = 4 h τ = 24 h	(200 FITS) IGCAR
6	SCRAM logic conventional (SLFIT)	All	1.0E − 7	FIT	λT (1)	T = 4 h	IGCAR
7	SCRAM logic pulse coded (PCSL)	All	1.0E − 7	Built-in	λT (1)	T = 4 h	IGCAR
8	SCRAM switch: (power gates)	Short	1.0E − 6	FIT	λT (1)	T = 4 h	IAEA-TECH-DOC-478 (1989)
9	Computation module	All	1.0E − 6	Continuously monitored	λT (1)	T = 4 h	Eide and Calley (1993)
10	CSR/DSR and Drive Assembly	Fail to insert or detach	3.0E − 5 /de	–	Q (3)	–	Eide and Calley (1993)
11	Real time computers						
	Software	–	1.0E − 4/de	–	Q(3)	–	IAEA.2000 (NS-G-1.1, 2000)
	Hardware	–	1.0E − 4/de	–	Q(3)	–	FBTR (Rao et al., 2003) (∼1E − 5/h × 24 h test)

13. Results

The results for SDS1 and SDS2 individually are given in Table 10. For global fault event, the failure probability on demand is 3.8E − 5 for SDS1 and 2.2E − 5 for SDS2. The corresponding values for local fault event is 2.5E − 5 and 4.4E − 4. With 20 demands per year for global faults, and 10^{-2} demands per year for local faults, the frequency of shutdown function failure for SDS1 is 7.6E − 4/y and for SDS2 it is 4.4E − 4/y.

The results for the SDS is shown in Table 11. The failure probability of actuation system is 3.4E − 8/demand (de) and the failure probability of RPS is 0.1E − 8 /de for global faults and 1.0E − 8 /de for local faults. The failure frequency of shutdown function is 0.7E − 6/ry.

14. Importance measures

To quantify the importance of a component, several measures of importance exist. Two basic measures for fault trees are RIF (Risk Increase Factor) and RDF (Risk Decrease Factor).

RIF is also expressed as

$$P_{\mathrm{RIF}}(i) = \frac{(P(S) \mid P(X_i) = 1)}{P(S)},$$

where $P(S)$ is the failure probability of the system and $P(X_i) = 1$ denote that the failure probability of the ith component is 1 (i.e., ith component becomes unavailable).

RDF is represented as

$$P_{\mathrm{RDF}}(i) = \frac{P(S)}{(P(S) \mid P(X_i) = 0)},$$

where $P(X_i) = 0$ denote that the failure probability of the ith component is 0 (i.e., ith component is made absolutely reliable).

Table 10
Results of reliability analysis for SDS1 and SDS2

System	Global fault			Local fault[a]			Unprotected event frequency (/y) $\lambda_S = (P^*_{SL}\lambda_L + P^*_{SG}\lambda_G)$
	Probability of failure on demand P_{SG}		Initiating event frequency λ_G (/y)	Probability of failure on demand P_{SL}		Initiating event frequency λ_L (/y)	
	AS	RPS		AS	RPS		
SDS1	3.1E − 6 3.8E − 5	3.5E − 5	20	3.1E − 6 2.5E − 5	2.2E − 5	1E − 2	7.6E − 4
SDS2	3.1E − 6 2.2E − 5	1.9E − 5	20	3.1E − 6 4.4E − 4	4.4E − 4	1E − 2	4.4E − 4

[a] Design basis blockage in any fuel SA (/ry), which is a Cat. III event.

Table 11
Results of reliability analysis for SDS

DBE	Event frequency (/y) λ	Probability of failure on demand			Unprotected event frequency (/y) $P_S\lambda$
		Actuation system (P_A)	RPS (P_R)	Total $P_S = (P_A + P_R)$	
Global fault	20	3.4E − 8	0.1 E − 8	3.5E − 8	7.0E − 07
Local fault	1E − 2	3.4E − 8	1.0E − 8	4.4E − 8	4.4E − 10
Total	20	–	–	–	7.0E − 07

Fussell–Vesely importance measure

$$P_{\mathrm{FV}}(i) = \frac{P(S/\mathrm{MCS}(i))}{P(S)},$$

where $P(S/\mathrm{MCS}(i))$ is the total system failure probability with only the minimal cut sets containing the ith basic event included.

The RDF, RIF and FV measure of the system due to various components for the two events, i.e., global fault and local faults indicate that the contribution of some of the components comes mainly from their corresponding common cause failures. This implies that the importance of such components is likely to be reduced when the common cause failures are reduced.

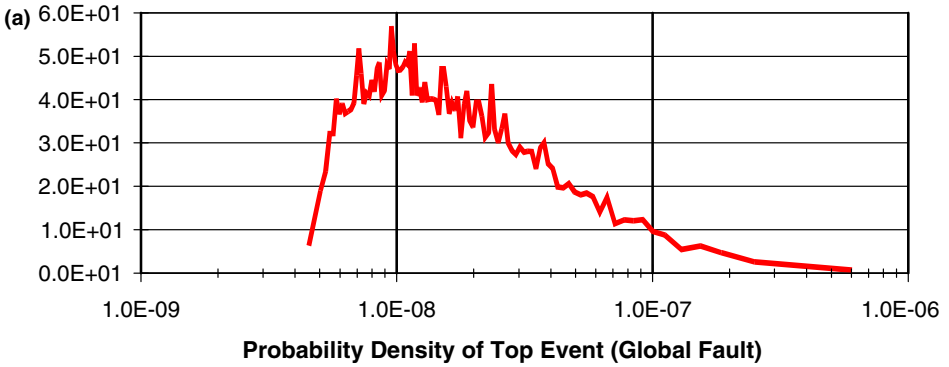
This analysis on importance measures indicates that the major components whose reliability needs to be improved are CCF of actuation part of SDS and SCRSW12CCF (CCF between SCRAM switches in system 1 and 2).

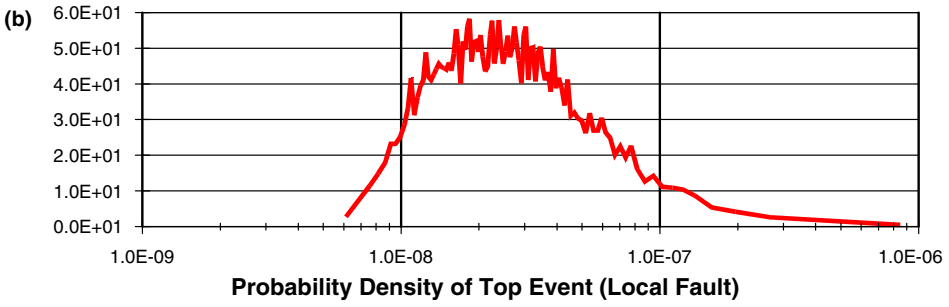
15. Sensitivity analysis

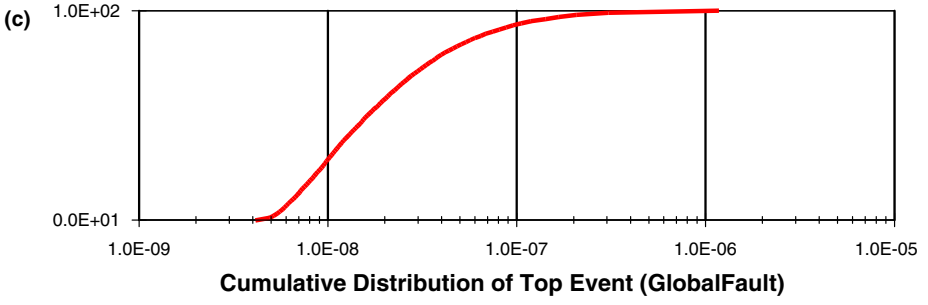
Sensitivity calculation of the basic events in the minimal cut set is carried out to find the top event unavailability responses to variations in basic input values of failure rates. The result of this analysis indicates the relative importance of individual component failure rates. The calculation is performed by calculating the ratio $Q_{\mathrm{TOP,U}}/Q_{\mathrm{TOP,L}}$ where $Q_{\mathrm{TOP,U}}$ is the top event unavailability when the basic event is assigned the nominal value multiplied by a sensitivity factor (default is 10) and $Q_{\mathrm{TOP,L}}$ is the top event unavailability when the basic event is assigned the nominal value divided by a sensitivity factor (default is 10). The results indicate that the CCF of actuation part of SDS is the most sensitive component.

16. Uncertainty analysis

Uncertainty analysis is carried out using Monte-Carlo simulation. For each basic event, failure rates are sampled from log–normal distribution. The distribution is constructed based on the Error Factor (EF) and median failure rate. The EF assigned based on available information and judgement range from 3 to 10. The sam-







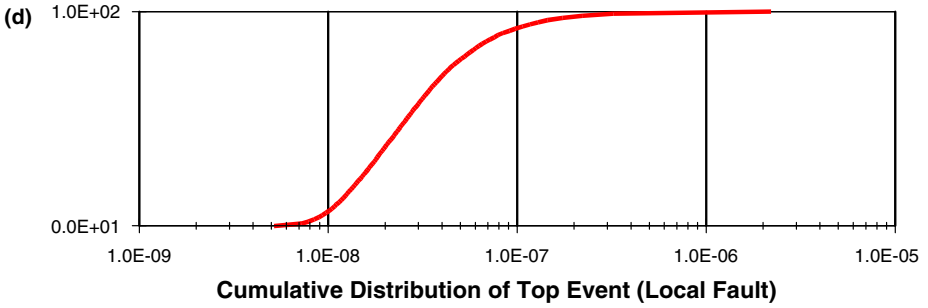


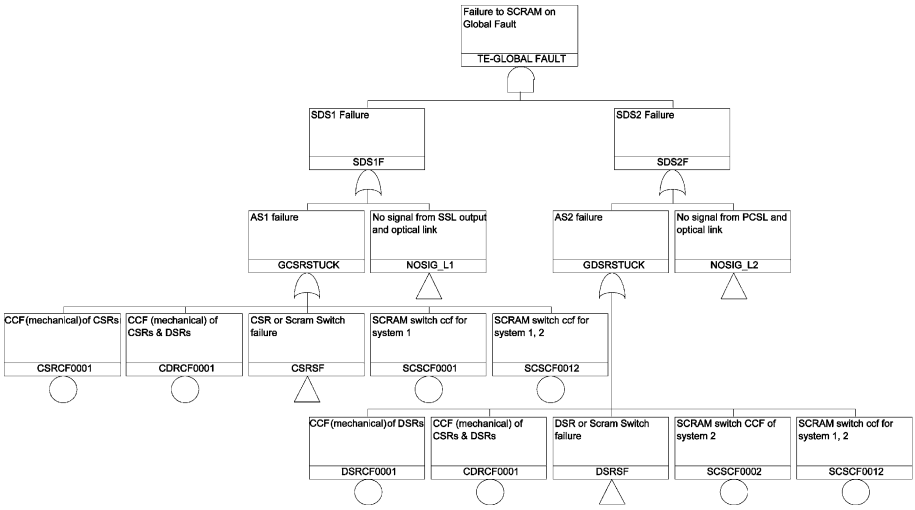
Fig. 4. (a) Probability density of top event (global fault), (b) probability density of top event (local fault), (c) cumulative distribution of top event (global fault), (d) cumulative distribution of top event (local fault).

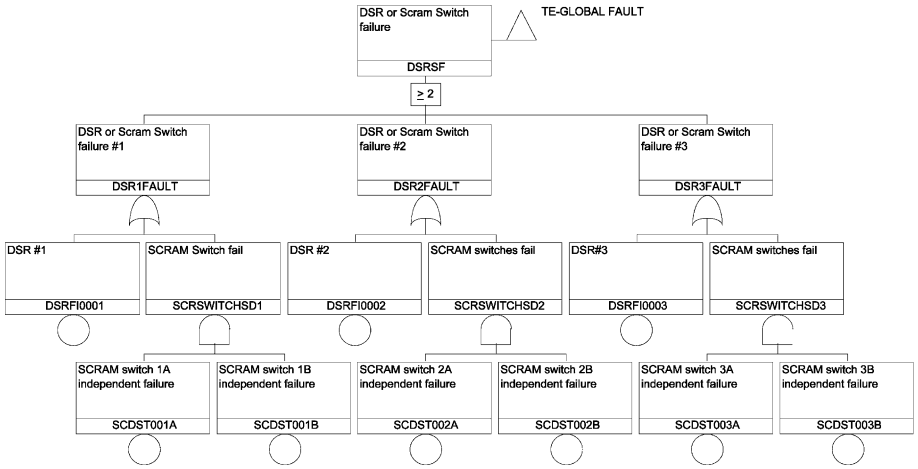
pled values are propagated to get the top event distribution. The probability distribution function and cumulative distribution function for global and local faults are given in Fig. 4(a)–(d). The number of simulations in this process is recommended to be at least 1000 in RISK SPECTRUM. For the shutdown system, the top event result is simulated 10,000 times and log–normal distribution is assumed for all the parameters. The analysis indicates that the top event result is uncertain by a factor of 4 for local fault and 5 for global fault.

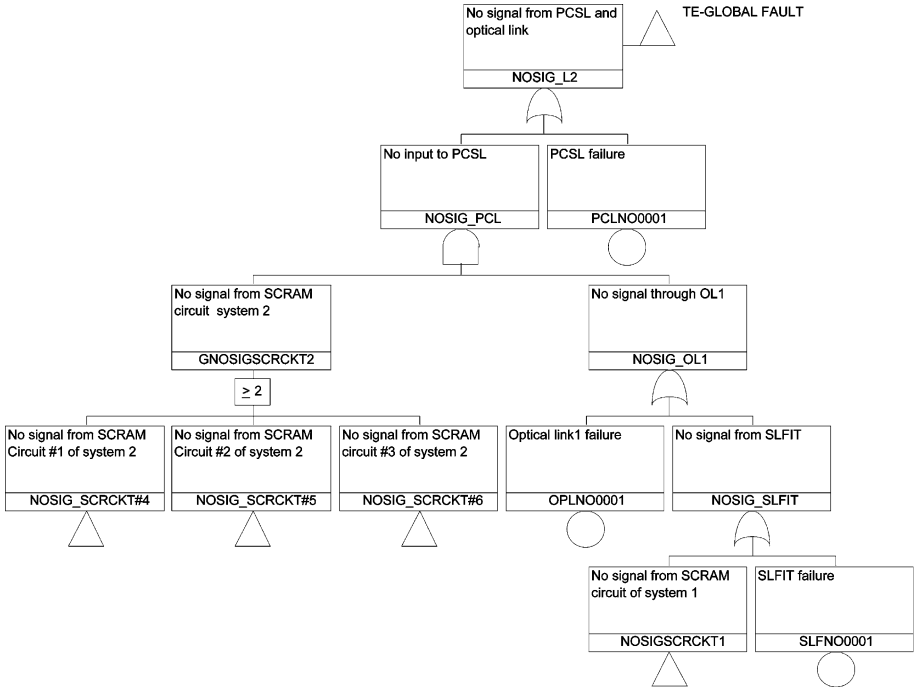
17. Conclusion

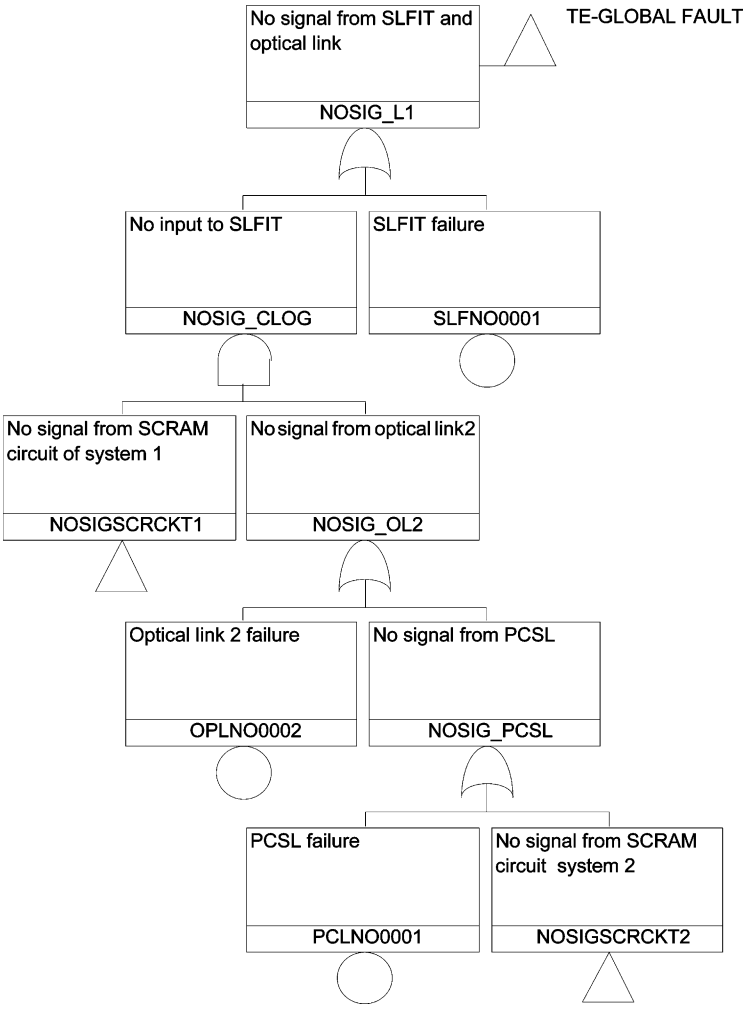
Reliability analysis of Shutdown System (SDS) is carried out using Fault Tree Analysis. The intent of the design has been on the simplicity, less number of components and high reliability. Diversity is provided for the sensors, signal-processing circuits, safety logic, drive mechanisms, release magnets and absorber rods to minimize common cause failures. Reliability analysis carried out using Fault Tree Analysis predicts a value of 3.5×10^{-8}/de for the failure of shutdown system in case of global fault events and 4.4×10^{-8}/de for local faults. Based on 20 de/y, the frequency of shutdown function failure is 0.7×10^{-6}/ry which meets the reliability target of 1×10^{-6}/ry. CCF of actuation part of SDS, and to a lesser extent CCF of electronic components, limits the reliability. The failure frequency of individual systems is $<1 \times 10^{-3}$/ry which also meets the safety criteria. Uncertainty analysis indicates a maximum error factor of 5 for the top event unavailability.

Appendix A. Fault trees for global fault event




DSR or Scram Switch failure
DSRSF
TE-GLOBAL FAULT
≥ 2
DSR or Scram Switch failure #1
DSR1FAULT
DSR or Scram Switch failure #2
DSR2FAULT
DSR or Scram Switch failure #3
DSR3FAULT
DSR #1
DSRFI0001
SCRAM Switch fail
SCRSWITCHSD1
DSR #2
DSRFI0002
SCRAM switches fail
SCRSWITCHSD2
DSR#3
DSRFI0003
SCRAM switches fail
SCRSWITCHSD3
SCRAM switch 1A independent failure
SCDST001A
SCRAM switch 1B independent failure
SCDST001B
SCRAM switch 2A independent failure
SCDST002A
SCRAM switch 2B independent failure
SCDST002B
SCRAM switch 3A independent failure
SCDST003A
SCRAM switch 3B independent failure
SCDST003B


No signal from PCSL and optical link
NOSIG_L2
TE-GLOBAL FAULT
No input to PCSL
NOSIG_PCL
PCSL failure
PCLNO0001
No signal from SCRAM circuit system 2
GNOSIGSCRCKT2
No signal through OL1
NOSIG_OL1
≥ 2
No signal from SCRAM Circuit #1 of system 2
NOSIG_SCRCKT#4
No signal from SCRAM Circuit #2 of system 2
NOSIG_SCRCKT#5
No signal from SCRAM circuit #3 of system 2
NOSIG_SCRCKT#6
Optical link1 failure
OPLNO0001
No signal from SLFIT
NOSIG_SLFIT
No signal from SCRAM circuit of system 1
NOSIGSCRCKT1
SLFIT failure
SLFNO0001



References

AERB Approved Document, 1990. Safety criteria for design of PFBR, April.

AERB Review Report on Safety Grade Decay Heat Removal System, 2002. AERB/PH/61090/8658/2k2, November.

Andrews, J.D., Moss, T.R., 1993. Reliability and Risk Assessment. Longman Scientific and Technical, London.

Bisseau, J., et al., 1982. Failure rate evaluation for different components operating in sodium based on operating experience of raphsodie and phenix reactors and test loops. In: International Topical Meeting on LMFBR Related Design, Lyon, vol. 1, Tech. Sess.1-5.

Edwards, G.T., Watson, I.A., 1979. A study of common mode failures. SRD-R-146, United Kingdom Atomic Energy Authority, July.

Eide, S.A., Calley, M.B., 1993. Generic component failure data base. In: Proceedings of the International Conference on PSA, vol. 2, FL, USA, p. 1175.

Ericson Jr., D.M., 1990. Analysis of Core Damage Frequency: Internal Events Methodology, NUREG/CR-4550, SAND86-2084, vol. 1, Rev. 1.

Humphreys, R.A., 1987. Check list method for evaluating the β factor, paper 2c/5. In: National Reliability Conference.

IAEA-TECDOC-930, 1997. Generic Component Reliability Data for Research Reactor PSA, IAEA, Vienna.

IAEA-TECH-DOC-478, 1989. Component Reliability Data for Probabilistic Safety Analysis, IAEA, Vienna.

IGCAR Internal Report, 1997. Conceptual Design of 500 Mwe Prototype Fast Breeder Reactor, December.

Kamal, S.A., Hill, D.J., 1993. Fault tree analysis of EBR II reactor shutdown system. In: Proceedings of Probabilistic Safety Assessment International Topical Meeting, vol.2, Florida, January, pp. 754–758.

Kasinathan, N., Vaidyanathan, G., Chetal, S.C., 1996. Conceptual design studies for core under cooling incidents, PFBR/RG/66040/DN/2010, November.

Kasinathan, N., Vaidyanathan, G., Chetal, S.C., 1997. Safety actions and reactor trip parameters, PFBR/RG/66040/DN/2019, January.

Mosleh, A., Felming, K.N., et al., 1988. Procedures for treating common cause failures in safety and reliability studies, NUREG/CR-4780. EPRI NP-5613, PLG-0547, January.

NS-G-1.1, 2000. Software for Computer Based Systems Important to Safety in Nuclear Power Plants, Safety Guide, IAEA Safety Standards series, IAEA, Vienna.

Rajan Babu, V., Govindarajan, S., Chetal, S.C., 1997. Design of control and safety rod and its drive mechanism of PFBR. In: Proceedings of Workshop on Reactor Shutdown System, IGCAR, Kalpakkam, 4–6 March.

Sasidhar Rao, B. et al., 2003. Core Temperature Monitoring System, SHINEG/EIG/EID/DES/2001/001, Rev.0.

Sanjay Alexis, A., 2000. Estimation of Beta Factor for reactor Shutdown System, PFBR/66300/DN-1002, July.

Swain, A.D., Guttmann, H.E., 1983. Handbook of Human Reliability Analysis, NUREG/CR-1278, USNRC.

Vijayashree, R., Govindarajan, S., Chetal, S.C., 1997. Design of diverse and safety rod and its drive mechanism of PFBR. In: Proceedings of Workshop on Reactor Shutdown System, IGCAR, Kalpakkam, 4–6 March.