

# 中国原子能科学研究院 第九届五四青年学术报告会文集

(反应堆工程和计算机技术应用部分)

(一九九五年五月)

中国原子能科学研究院科学技术委员会

中国原子能科学研究院团委

中国原子能科学研究院科技信息部

一九九五年六月

# CEFR安全棒停堆系统可靠性分析

王 国 强

(反应堆工程设计研究所)

可靠性做为—门学科始于第二次世界大战期间(1940—1945),首先运用于军事领域,到1960年,美国陆续制定了军用规格和标准,并成为今日可靠性标准体系的基础. 1975年代号为WASH-1400的'反应堆安全研究'报告的发表被称为概率安全评价发展的里程碑. 1985年英国专家提出,把PSA做为核电站概率安全评价的专用术语. PSA技术采用系统可靠性(如故障树、事件树方法)和概率风险(即事故发生概率与该事故后果的乘积)分析方法,对复杂系统的各种可能事故的发生和发展过程进行全面分析.

经国际原子能机构(IAEA)专家组全面综合鉴定过的大型软件系统程序THPSA(SETS程序的微机版本)具有良好的数据管理系统,人机界面良好,可以完成核电站概率安全评价第一级分析的全部任务,即系统故障树分析和事故序列分析.

本文选用故障树分析方法(FTA),对中国实验快堆(CEFR)安全棒停堆系统的系统故障模式、顶事件(即两根安全棒均不能插入堆芯)发生的概率及不确定性和部件重要度进行了具体分析.

## 1. CEFR安全棒停堆系统的描述.

中国实验快堆(CEFR)设计热功率为65MW,实验电功率为20MW. 预计2000年前后投入运行. 把CEFR安全棒停堆系统的功能和组成分别描述如下.

### 1.1 CEFR停堆系统的功能.

虽然CEFR在设计和未来建造时将采取一系列的安全措施,但由于设备的老化、磨损或操作错误等原因,反应堆在运行中还可能出现某些故障. 为了防止故障扩大以及减轻反应堆事故时所造成的后果,CEFR设置了两套停堆系统,即第一停堆系统(PSS)和第二停堆

系统 (SSS) 或称安全棒停堆系统. PSS的功能包括安全停堆、功率调节、温度及燃耗补偿以及换料和其它因素所引起的反应性变化的补偿. SSS的功能是安全停堆. 两套系统都满足卡棒准则: 即当两系统中效率最大的一根控制棒组件被卡住时, 两系统中任何一套系统都能使反应堆从任何一个工况达到热停堆状态 ( $400^{\circ}\text{C}$ ). 两套系统能使反应堆达到冷停堆状态并保持足够的停堆深度, 两套系统是独立动作的, 即任何一套系统的控制能力不受另一套系统运行情况 (正常运行和故障) 的影响. 一旦出现有损于反应堆安全的异常工况, 上述两套停堆系统即能执行保护反应堆的动作, 立即消除事故隐患, 从而保证反应堆及其系统、运行人员和周围环境的安全.

## 1.2 CEFR安全棒停堆系统的组成.

安全棒停堆系统包括保护系统、控制棒驱动系统 (包括控制棒组件) 及有关辅助系统.

### 1.2.1 CEFR安全棒驱动系统的组成.

CEFR由8根控制棒组件控制, 其中2根安全棒, 2根调节棒, 4根补偿棒. 控制棒组件由导向部件和吸收体部件组成, 其外形尺寸和燃料组件是一致的. 8根控制棒在堆芯中的布置如图1-1所示. 其中两根安全棒的价值均为  $2.05\% (\Delta k/k)$ , 总效率为  $4.177\% (\Delta k/k)$ , 下插到堆芯底部约需0.7秒. (注: 满功率平衡装载剩余反应性为  $1.59\% (\Delta k/k)$ )

2根安全棒分别由两个驱动机构驱动, 每个驱动机构包括两个运动链: 主轴传动链和抓手传动链.

主轴传动装置由步进电机、上下减速器、传动轴、电磁离合器、齿条付、抓爪轴、加速弹簧、减震弹簧、位置发送器、终端和行程开关组成.

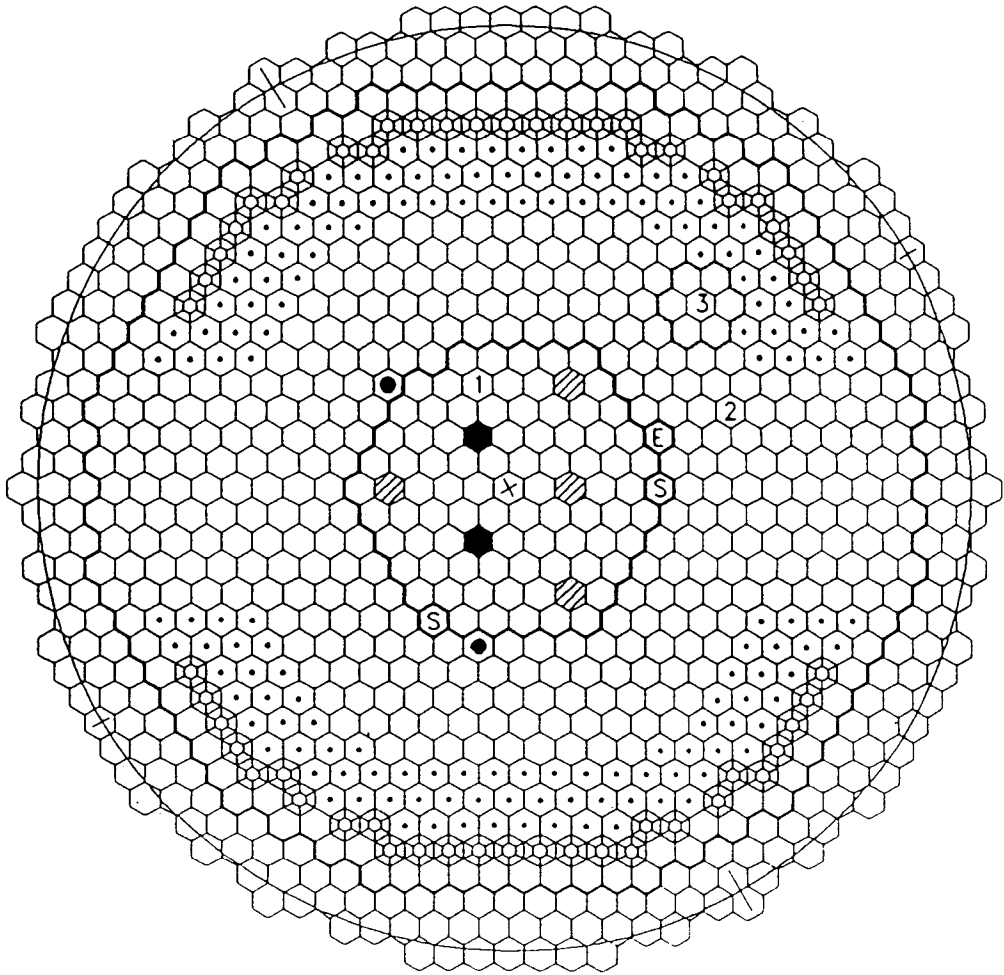
抓手传动装置由步进电机、减速器、旋转套筒、抓手操纵杆、敏感元件和发送器组成.

### 1.2.2 CEFR保护系统组成

CEFR保护系统包括下列几部分:

- 核测量通道 (探测器和仪表)
- 过程测量通道 (一次和二次仪表)

- 安全逻辑装置
- 安全旁通装置
- 安全报警装置
- 手动投入及触发单元
- 安全断路器
- 安全联锁单元
- 在役检验单元



① 燃料组件	82	▨ 补偿棒	4
② 反射层组件	378	● 调节棒	2
③ 屏蔽层组件	152	⊙ S 中子源	2
⊙ 乏燃料储存	54	⊙ E 实验装置	1
● 安全棒	2	③ 实验回路	7

图1-1 堆芯布置

CEFR保护系统框图如附图1所示。在该保护系统中,对同一个保护变量设置了三个独立的监测装置,每个监测装置将始自传感器,终至仪器仪表的输出。保护动作限值在监测装置定值单元上设定。同一个监测装置的输出,送往保护系统的两个冗余通道的安全逻辑装置,并进行三取二的逻辑处理。每个安全逻辑装置控制3X2个断路器。三组断路器分别控制1#安全棒、2#安全棒和控制棒电磁离合器的驱动电源。此外,还设有三个紧急停堆按钮,其中一个设在备用停堆点,两个设在主控室操纵台。这三个停堆按钮与上述断路器一起控制安全棒和控制棒电磁离合器的驱动电源。当在紧急情况下按下停堆按钮或表1-1中的任一停堆信号发出时,保护系统立即使

表1-1 CEFR自动保护参数

- ★中子注量率 (GB)
- ★反应堆周期 (ZQ)
- ★一回路钠冷却剂出口温度 (CW1)
- ★一回路钠冷却剂流量 (LL1)
- ★一回路钠冷却剂液位 (YW1)
- ★堆芯出口温度 (DW)
- ★一次钠泵转速低或失电 (PS1)
- ★二次钠进出口温差或出口温度 (WC)
- ★二回路钠流量 (LL2)
- ★二次钠泵转速低或失电 (PS2)
- ★蒸汽回路流量 (ZL)
- ★外电网失电 (SD)
- ★二次钠冷却剂泄漏引起较大钠燃烧 (NH)
- ★地震加速度超过规定值 (DZ)

磁铁释放,使两根安全棒靠自重和顶端加速弹簧的作用在0.7秒的时间内下插到底,从而关闭反应堆(所有控制棒作为第一套停堆系统先开始下插,但下降速度较安全棒慢(约需1.5秒))。

## 2. 故障树的建造.

### 2.1 顶事件的定义及成功准则

当要求关闭反应堆的信号到达控制保护系统时,而不能使反应堆的安全棒插入堆芯,是不希望发生的事件,也即本文所研究的顶事件.

顶事件定义为: '安全棒A、B均不能插入堆芯'.

成功准则描述为: 当要求关闭反应堆的信号到达控制保护系统时,或在紧急情况下,手动按下停堆按钮时,两根安全棒至少有一根插入堆芯,从而关闭反应堆.

### 2.2 CEFR安全棒停堆系统故障树的建造

图2-1为简化的功能事件树. '停堆系统动作关闭反应堆'在任何一个功能事件树中,一般为排在前面的顶事件(如图2-1中箭头所示),其它事件(如堆芯冷却等)排在其后.

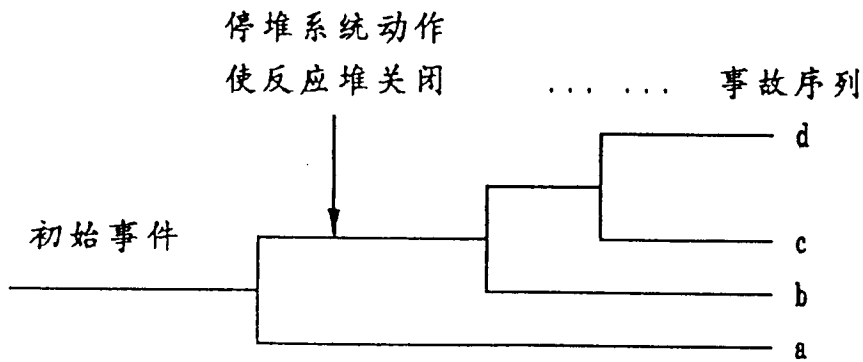


图2-1 功能事件树

显然,在进行事故序列分析之前,首先应对每一个顶事件进行故障树分析.

下面根据安全棒停堆系统(即保护系统和安全棒驱动系统)的组成,及有关设计人员和经验丰富的运行人员提出的建议建造故障树.

首先把CEFR保护系统的控制电路图进行简化,简化后的电路图如图2-2所示。

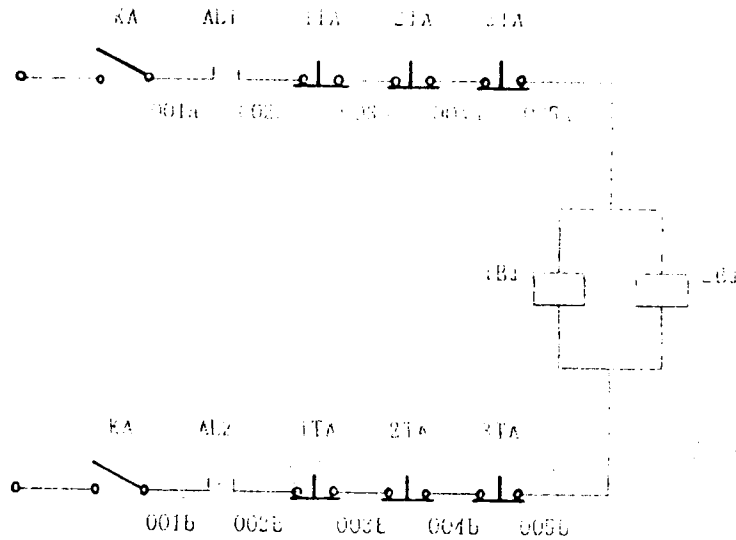


图2-2 CEFR保护系统控制电路图

要建造故障树的顶事件是'两根安全棒均不能插入堆芯',它是一个或门的顶结构,直接原因是'安全棒停堆系统故障 A、B棒不能插入堆芯'或者'共同外部原因使安全棒机械卡住'。前者的直接原因是'A棒不能插入堆芯'和'B棒不能插入堆芯'。'A(B)棒不能插入堆芯'的直接原因是'A(B)棒机械故障'或'A(B)棒导管堵'或'A(B)棒导管顶端加速弹簧失效'或'A(B)磁铁有磁性'。后者的直接原因是'磁铁线圈有电流通过'或'线圈有剩磁'。前者的直接原因即图2-2中电流流过接点005a(b)的导通条件。然后,逐点分析点004a(b)至001a(b)的导通条件,即分析出故障树建造的全过程。按上述建树思想编写SETS用户程序并通过THPSA程序中的SETS模块执行此用户程序,再编写FTD模块的用户程序并执行此程序,生成的故障树通过FTPE模块用打印机输出。画出的故障树如图2-3所示。

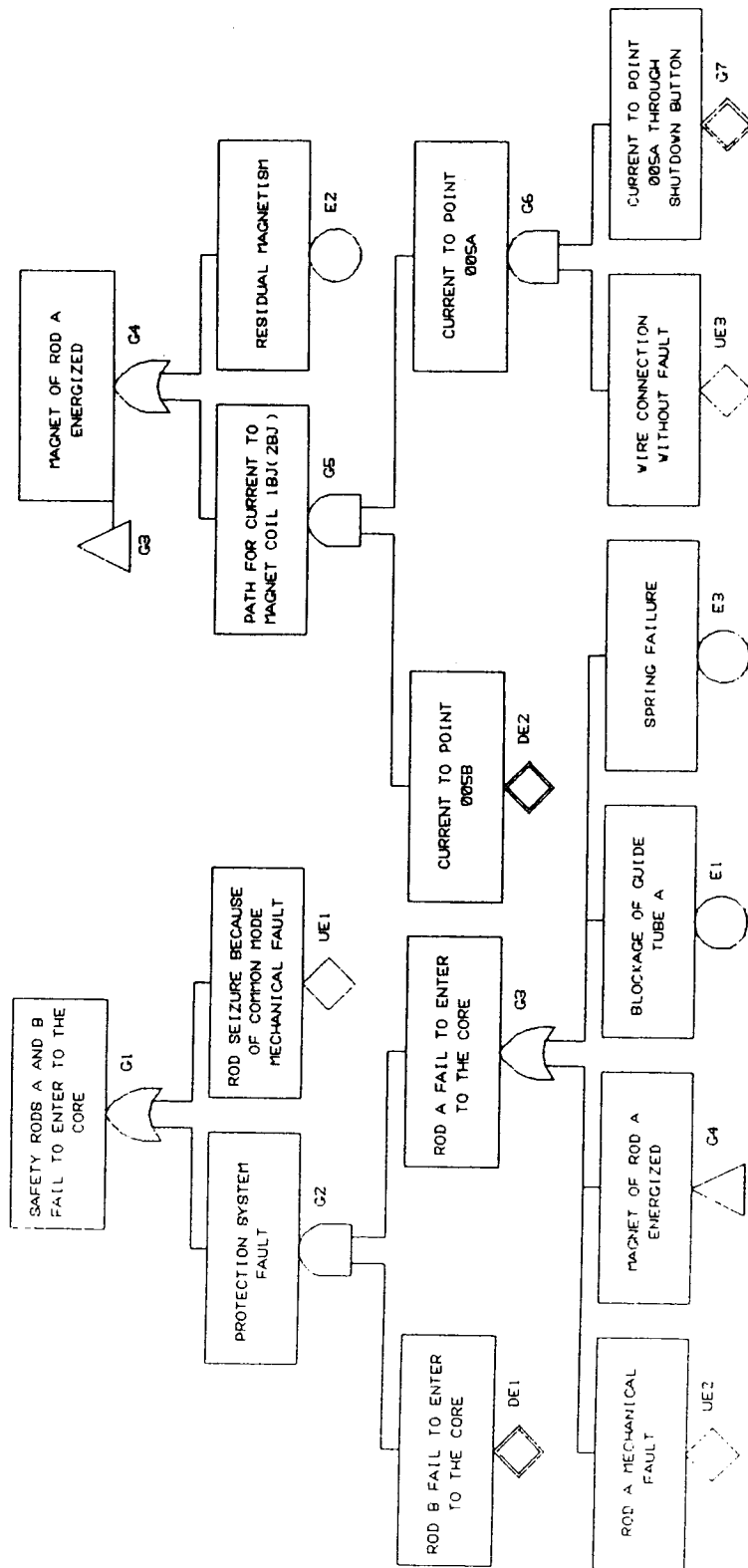


图 2-3 CEFR 安全棒停堆系统故障树(1)



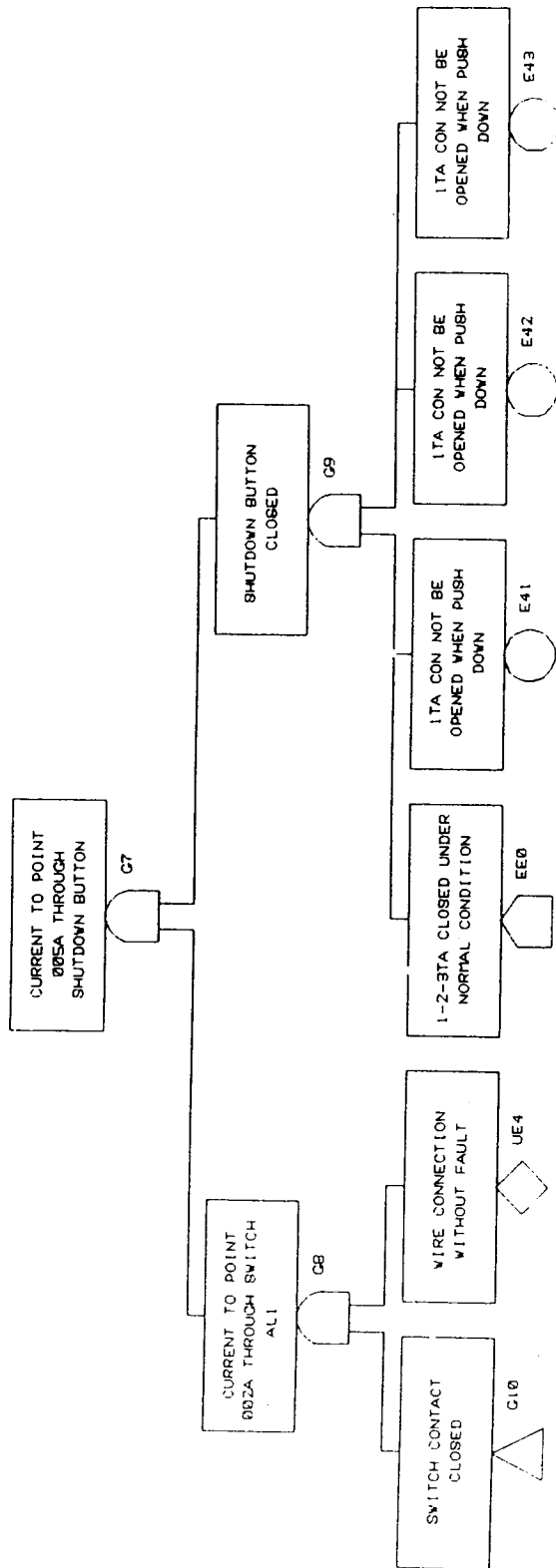


图 2-3 CEFR 安全棒停堆系统故障树(2)

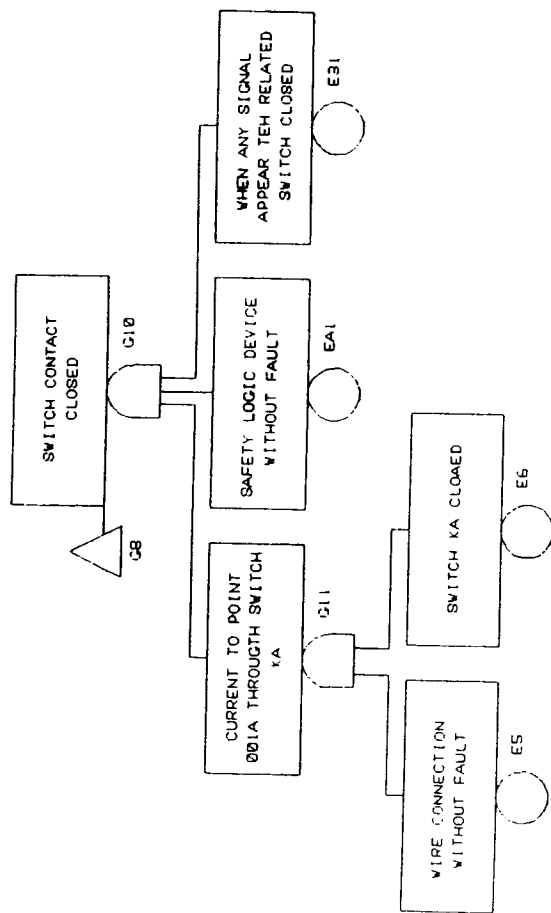


图 2-3 CEFR 安全棒停堆系统故障树(3)

### 3. 故障树分析及评价.

#### 3.1 故障树的定性分析及最小割集方程.

本文所建造的故障树为正规故障树, 它仅由或门和与门组成, 所有底事件都是统计独立的. 通过SETS程序生成的最小割集方程如下:

$$G1 = E2 \cdot E1A + E2 \cdot UE2A + E3 \cdot E1A + E3 \cdot UE2A + E1 \cdot E1A \\ + E1 \cdot UE2A + UE2 \cdot UE2A + UE2 \cdot E1A + E1 \cdot E3A \\ + UE2 \cdot E3A + E2 \cdot E2A + E1 \cdot E2A + UE2 \cdot E2A + UE1$$

方程右边每一个乘积项即一个最小割集, 所有最小割集组成系统的全部故障模式(或称故障谱). 当单个停堆信号发出时, 对应测量通道发生故障, 是对顶事件发生概率贡献最大的失效模式. 本文仅对此模式进行定量分析.

#### 3.2 故障树定量分析.

##### 3.2.1 基本事件失效数据的获得.

对有运行历史的反应堆系统进行可靠性分析, 所需基本事件失效率数据, 可在反应堆运行过程中用统计方法获得. 然后换算成失效分布概率. 由于CEFR尚在设计阶段, 显然无法通过上述方法获得数据. 查阅有关资料并经有关专家审定后, 把基本事件失效分布概率列于表3-1中.

表3-1 基本事件失效概率

编号	基本事件名称	失效概率	误差因子f
1	共因机械卡棒(外部)	1.1E-07	3.0
2	棒机械故障	4.6E-03	3.0
3	加速弹簧失效	2.0E-03	3.0
4	剩磁	2.7E-04	3.0
5	导管堵	1.0E-05	3.0
6	安全逻辑装置故障	1.0E-03	3.0
7	导线故障	1.7E-03	3.0
8	任一停堆信号发出 后电子开关故障闭	3.0E-04	3.0

表3-1中误差因子f说明了数据的不确定性范围. 其定义如下:

$$\int_{x_{0.5}/f}^{x_{0.5} \cdot f} f(x) dx = 90\%$$

其中,  $f(x)$ ——为失效密度函数.

$x_{0.5}$ ——为对数正态分布50%的概率分位点.

### 3.2.2 顶事件发生概率及不确定性分析.

编写用户程序后通过THPSA程序的UPIM模块用蒙特卡罗法,对建造好的故障树进行不确定性分析.分析结果可以通过PRNSET模块打印输出.

编写FORTRAN语言程序对输出结果进行处理,再用GRAPHER软件把生成的数据文件中的数据结果拟合成曲线.即得到顶事件失效密度函数 $f(x)$ 及失效分布概率函数 $F(x)$ 的分布图.

故障树中顶事件失效密度函数 $f(x)$ 及失效分布概率函数 $F(x)$ 分布图如图3-1和3-2所示.通过UPIM模块用对数正态分布拟合求出顶事件发生概率的均值为:  $0.7586E-04$ .

置信度95%的置信区间为:  $(0.1798E-04, 0.1911E-03)$ .

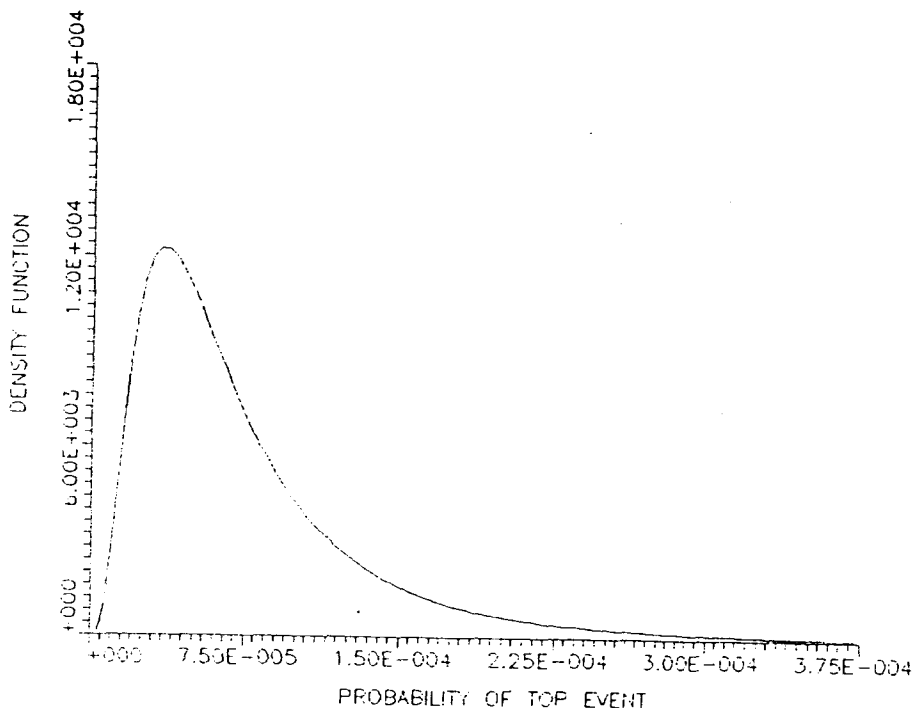


图3-1 失效密度函数 $f(x)$ 分布图

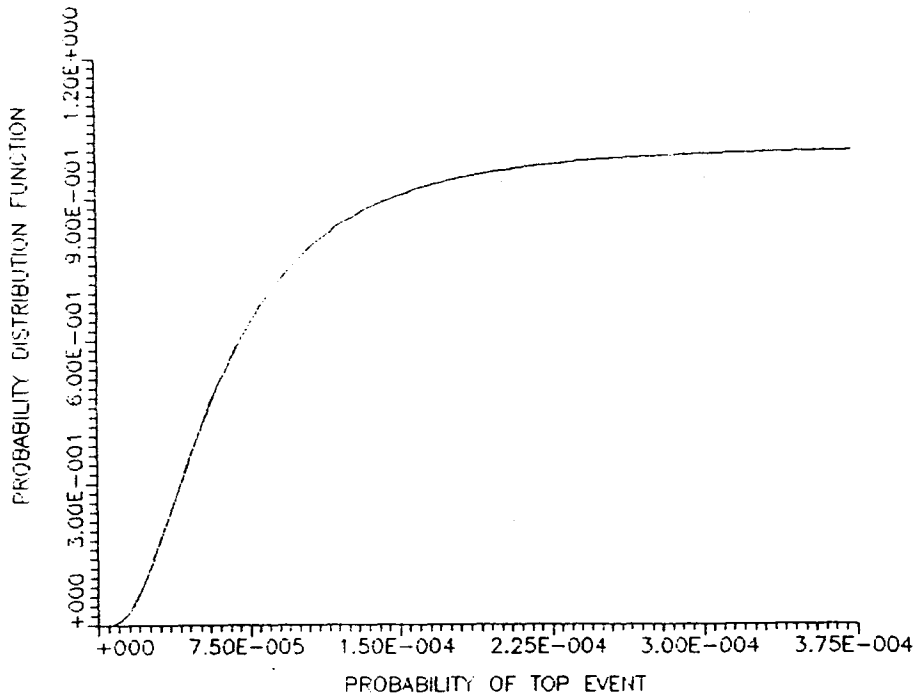


图3-2 失效分布概率函数F(x)分布图

分析上述计算结果可以看出：两根安全棒均不能插入堆芯的概率是很低的，即此设计方案满足可靠性目标的要求。

### 3.2.3 重要度分析.

#### 3.2.3.1 重要度的定义.

重要度是一个部件或者系统的割集发生失效时对顶事件发生概率的贡献，它是时间、部件的可靠性参数以及系统结构的函数。

部件的概率重要度、结构重要度及关键重要度分别定义如下：

$$\textcircled{\circ} \text{ 部件概率重要度: } I^{PR}_i = \frac{g(Q)}{Q_i} \quad \text{————— 3-1}$$

$$\textcircled{\circ} \text{ 部件结构重要度: } I^{ST}_i = \frac{g(Q)}{Q_i} \quad \text{————— 3-2}$$

$$\textcircled{\circ} \text{ 部件关键重要度: } I^{CR}_i = \frac{g(Q)}{Q_i} \cdot \frac{Q_i}{g(Q)} \quad \text{————— 3-3}$$

其中,  $I$  —— 为重要度.

$i$  —— 为部件  $i$ .

$g(Q)$  —— 为故障树的结构函数.

$Q$  —— 为失效概率矢量 ( $Q_1, Q_2, \dots, Q_1, \dots, Q_n$ ).

$Q_i$  —— 为部件  $i$  的失效概率.

### 3.2.3.2 SETS程序计算结果.

THPSA程序的UPIM模块,可以计算部件的概率重要度、结构重要度和关键重要度.通过UPIM模块执行有关的用户程序,计算结果通过PRNSET模块打印输出.计算结果列于表3-2中.

表3-2 部件重要度表

编号	部件名称	概率重要度	结构重要度	关键重要度
1	棒机械故障 (UE2)	0.860E-02	0.667E+00	0.200E+01
2	加速弹簧失效 (E1)	0.860E-02	0.290E+00	0.200E+01
3	剩磁 (E2)	0.859E-02	0.391E-01	0.150E+01
4	外部共因机械卡棒 (UE1)	0.100E+01	0.186E-02	0.100E+01

根据表3-2中的数据,画出关键重要度的直方图如图3-3所示.

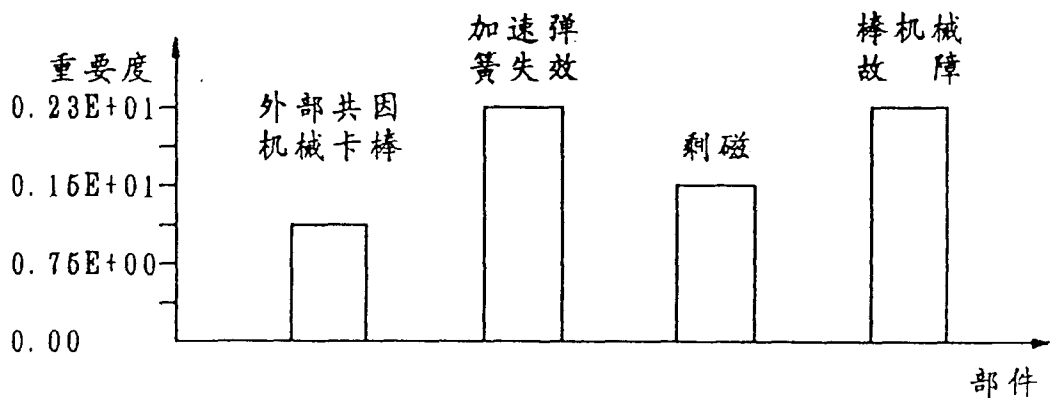


图3-3 部件关键重要度直方图

从重要度直方图可以看出:棒机械故障、加速弹簧失效和剩磁是对顶事件发生概率贡献最大的事件.

#### 4. 结论.

(1) 根据国家核安全局《核电厂安全导则》中“核电厂保护系统及有关设施”(HAF0203)一章的要求,本文用THPSA程序对安全棒停堆系统进行了故障树分析,分析结果满足可靠性目标的要求.

(2) CEFR保护系统两根安全棒不能插入堆芯的概率为 $0.758E-4$ .因此,安全棒停堆系统的可靠性是很高的.

(3) 从重要度分析可以看出,棒机械故障、加速弹簧失效和剩磁是对顶事件发生概率贡献最大的事件.上述事件的相应部件即安全棒停堆系统中的薄弱环节.提高这些部件的可靠性,对安全棒停堆系统可靠性与安全性的提高最有效.

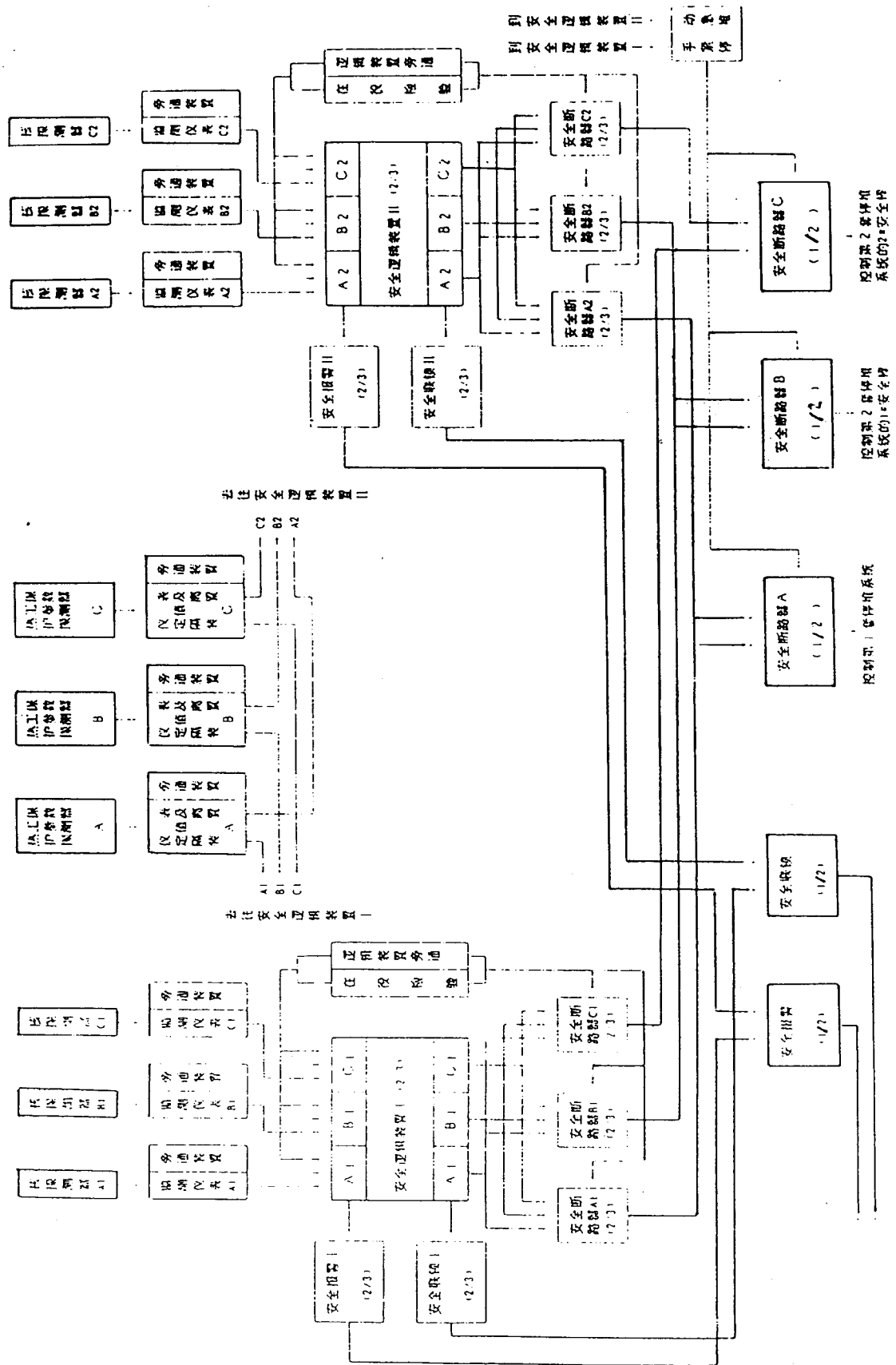
(4) 可靠性分析的实际意义还在于,通过可靠性分析,暴露系统的薄弱环节,进行合理的可靠性分配.给设计者提供必要的数据,使设备或系统在设计上达到执行其预期功能、可靠性和费用之间的综合平衡,从而得到最佳设计.

#### 5. 未来任务展望.

(1) THPSA (SETS程序微机版)程序可以完成中国实验快堆(CEFR)概率安全评价第一级分析的全部任务.但有关数据需要从俄罗斯BN-600或其它类似的反应堆上获得.

(2) 在不断总结经验和学习的基础上,结合“九·五”可靠性科研规划项目,可以进行一些开发性的工作或利用有关程序对系统和设备进行可靠性分析.

(3) 经验表明,一个较完整的数据库对可靠性分析工作是十分必要的.因此,结合快堆和“九·五”可靠性科研规划的有关项目建造数据库是一项具有重要意义而又十分繁重的工作.



附图 1 CEFR保护系统框图



## 参考文献

- (1) 李兆桓编著, 概率安全分析讲义, 原子能科学研究院, 1987年9月.
- (2) 谢钢等译, SETS用户程序手册, 清华大学, 1986年3月.
- (3) 黄祥瑞编著, 可靠性工程, 清华大学出版社, 1990年10月.
- (4) 第27卷第4期, 原子能科学技术, 原子能出版社, 1993年4月.
- (5) 田和春等编著, 中国实验快堆技术方案, 1994年3月.
- (6) 1-4集, 快堆专辑, 中国核学会, 1991年9月.
- (7) 国家核安全局政策法规处编, 核电厂安全导则汇编, 中国法制出版社, 1992年3月.
- (8) Huang Xiangrui, Fault Tree Analysis of the Pool Type Reactor Scram System of TsingHua University, IAEA-SR-111/8, 1985.
- (9) IAEA-TECDOC-478, Component Reliability Data for Use in Probabilistic Safety Assessment, IAEA, Vienna, 1988.
- (10) GRS-56, Risk-Orited Analysis of the SNR-300, 1984.