第24卷第1期 原子能科学技术 Vol.24,No. 1
1990年1月 Atomic Energy Science and Technology Jan. 1990

核电站概率风险评价中相依故障分析方法评述

周法清

(上海交通大学动力机械系)

一、概 述

根据单一故障的安全设计准则，核电站安全系统是按冗余原则设计的。随着冗余度的增加，可以使部件的独立故障对系统故障的贡献逐渐减少，然而，多个部件同时故障导致系统故障的贡献呈增加的趋势。对有些系统来说,后者有时可起到决定性的作用。根据核电站概率风险评价研究和安全系统可靠性分析,可以展望,相依故障将成为导致核电站事故的重要因素。例如，在 Zion 和 Indian Point 两座核电站的 PRA 资料中指出：对风险起决定作用的初始事件是地震、火灾和小破口失水事故。象地震和火灾那样的外部事件是众所周知的相依故障的触发原因。

按相依故障发生的机理，它可分共因、共模和因果故障三种方式。共因故障系指由单一原因引起几个设备或系统同时发生故障；共模故障是指一些相同的设备或系统按照相同的故障模式同时发生故障；传播型故障是指一个部件或系统故障，它将导致其它部件或系统也发生故障。

对核电站风险分析者来说，往往需要了解核电站各系统之间、系统内各部件间、系统与触发事件之间存在的相依关系。因而相依故障又可分为共因触发事件、系统间的相依、和部件间相依三种类型。系统间相依包括功能相依、公用设备相依、实体作用和人为作用等。

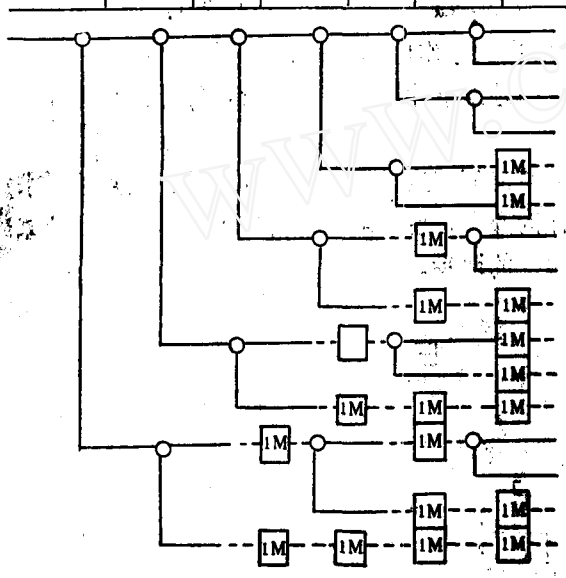
根据文献[1]报导，滥用故障模式独立的假设，可导致过低估计系统故障频率达几个量级。为此，预测核电站内系统和设备的相依故障是十分重要的。近十多年来，国外资料已公布了许多有关相依故障的分析模型，从形式上大体可归纳为显式模型和参数模型两大类。事件树、故障树、因果表等属显式模型；β 因子法、基本参数模型、多重希腊字母模型、两项式故障率模型等属参数模型。鉴于系统中相依事件的复杂性和故障类型的多样性，因而在 PRA 研究和系统可靠性分析中，需根据具体情况选用不同的模型。

二、显式模型

1. 事件树分析模型[2]

在 PRA 中，应用事件树分析方法分析事故序列中涉及系统相依故障发生的概率是十分有用的。它可用来分析系统间的功能相依、公共设备相依、实体作用和人为作用。通过下列来说明。

初因事件为 I_E，为确保电站安全，假设初因事件发生后需要堆芯应急冷却系统(ECCS)、辅助给水系统(AFWS)和安全壳通风系统(FC)投入工作。并且这三个系统都需要d-c，a-c电源和供应水源作支撑系统。这些系统都由A和B两个子系统组成，在功能上a-c依赖于d-c，供应水源依赖于d-c和a-c电源。由支撑系统组成的前侧系统的事件树示于图1。



初始事件发生	d-c电源投入		a-c电源投入		供应水操作		序列	序列影响矢量						支持系统状态	单值影响矢量					
								ECCS		AFWS		FC			ECCS		AFWS		FC	
	通道A	通道B	分支A	分支B	系列A	系列B	(j)	A	B	A	B	A	B	(K)	A	B	A	B	A	B
							1	0	0	0	0	0	0	1	0	0	0	0	0	0
							2	0	1	0	1	0	1	2	0	1	0	1	0	1
							3	1	0	1	0	1	0	3	1	0	1	0	1	0
							4	1	1	1	1	1	1	4	1	1	1	1	1	1
							5	0	1	0	1	0	1							
							6	1	1	1	1	1	1							
							7	1	0	1	0	1	0							
							8	1	1	1	1	1	1							
							9	0	1	0	1	0	1							
							10	0	1	0	1	0	1							
							11	1	1	1	1	1	1							
							12	1	1	1	1	1	1							
							13	1	0	1	0	1	0							
							14	1	1	1	1	1	1							
							15	1	1	1	1	1	1							
							16	1	1	1	1	1	1							

1M代表不可能事件

图 1 支撑系统事件树

Fig. 1 Event tree of the support system

事件树中每个支撑系统成功与故障状态的综合影响，是用事故序列的影响矢量代表，相同状态的事故序列影响可用单值影响矢量表示。单值影响矢量K的频率为：

$$\phi(I_K/I_E)=\sum_j \phi(I_{jK}/I_E) \tag{1}$$

式中：$\phi(I_K/I_E)$为发生初因事件I_E时单值影响矢量K的总频率；$\phi(I_{jK}/I_E)$是第j个事件序列频率，在一定的初因条件下，其影响矢量与单值影响矢量I_K相同。

前侧系统事件树l的总频率为

$$\phi(l)=\phi(I_E)\sum_{K=1}\phi(I_K/I_E)\phi(l/I_K,I_E) \tag{2}$$

式中$\phi(I_E)$为初因事件频率；$\phi(l/I_K,\ I_E)$为给定初因事件I_E和支撑系统状态K的条件下，前侧系统事件树l的频率。

在Zion电站的PRA中就应用该法分析了安全系统对电源的相依性。近来又把该法併入GO程序，它能根据电站各系统内部连接的GO模型自动构造事件树，给每一序列指定一个影响矢量，并按公式(1)叠加，利用计算机辅助技术分析系统内的相依性，大大

简化前侧系统事件树分析。

2. 故障树分析方法

(1) 假事件法[3]。用此法分析系统相依故障时，首先按常规法建造系统的故障树，然后分析故障树所含事件的相依性，找出能促使系统或部件发生相依故障的共同触发事件，确定基本事件对共因触发事件的相依程度(称假事件)。假事件法就是把每个共因触发事件与相应的假事件以基本事件方式画在故障树中，如图 2 所示。图 2 (a)是不考虑共因影响，则事件 x 的布尔表达式，为 $x=R=R_1(R_2UR_3)$；若事件 x 受共因触发事件 A 的影响，其影响程度为 E(见图 2 (b))，则 x 的布尔表达式为：$x=AE+R_1(R_2UR_3)$；如果事件 x 强烈依赖于共因触发事件，那末 $P(E)=1$，考虑共因作用的故障树示于图 2 (c)。

事件 x 可以是系统、部件和二次事件。共因触发事件包括地震、火灾等外部事件和实体作用及人为作用等内部事件。

假事件法简单、易行，在共因事件较少的情况下，这是一种可取的方法。缺点是寻求条件概率困难。另外，共同触发事件和假事件的介入，使故障树变得庞大，这对一个原来就比较复杂的系统，会使计算量猛增到无法实现的地步。

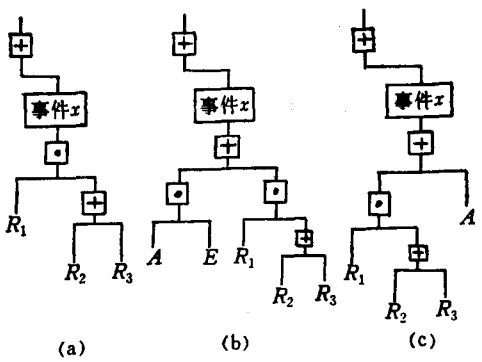


图 2 引入共因因子和假事件后的故障树

Fig. 2 Fault tree interting the causative factor and pseudo event

(2) 共同原因法[4]。此法就是从一组对系统产生同样影响的共因触发事件抽象出来的一般特性，如地震、飞弹等共同触发事件用“冲击”这一共性原因概括。该法不把共因事件介入故障树，按常规方法求出故障树的最小割集(MCS)，然后对 MCS 中的基本事件进行相依性分析。凡 MCS 中所含的基本事件都对某一共性原因敏感，且这些事件又都处在该共性原因的同一个影响区中，这样的割集称共因目标集。

本文通过实例说明寻找共因目标集的步骤。该例共有 12 个基本事例，经 FTA 求得最小割集有 x_1，x_4，x_6，x_3x_{12}，x_2x_{10}，x_2x_{11}，x_2x_3，x_2x_5，x_2x_9，x_5x_7，$x_7x_8x_{10}$，$x_3x_7x_8$，$x_7x_8x_9$等。

A．将系统所占空间划分成若干区域，决定每一区域内所受到的共因作用(表 1)，共因原因可多于一个。

B．决定各基本事件所处的物理位置(见表 2)。

C．根据表 1 和 2 决定受共因作用的基本事件，得敏感事件表 3 。例如，对 I_1来说，

表 1 共 性 原 因 域

Table 1 Generic cause domain

共 性 原 因	共 性 原 因 的 域
I(冲击)	I_1: 102, 104 I_2: 101, 103, 105, 199 I_3: 106
S(应力)	S_1: 103, 105, 106 S_2: 199 S_3: 101, 102, 104
T(温度)	T_1: 106 T_2: 101, 102, 103, 104, 105, 199
V(振动)	V_1: 102, 104, 106 V_2: 101, 103, 105, 199

表 2 基本事件的敏感性

Table 2 Susceptibility of the basic events

基 本 事 件	共性原因敏感性	物 理 位 置
1	I, S	101
2	I, S	105
3	I, T	104
4	S, T	104
5	T, V	102
6	I, V	102
7	I, V, S	105
8	I, V, T	105
9	S	199
10	I, V, S, T	106
11	S, T	103
12	T	104

表 3 敏感事件共同位置

Table 3 Common location for susceptibility events

共 同 位 置	敏 感 事 件
I_1	3,6
I_2	1,2,7,8
I_3	10
S_1	2,7,10,11
S_2	9
S_3	1,4
T_1	10
T_2	3,4,5,8,11,12
V_1	5,6,10
V_2	7,8

由表1受I_1影响的区域为102和104，由表2处在102区域内对I_1敏感事件为6，处在104区域内对I_1敏感事件为3。

D．分析求出的最小割集，如果割集内各基本事件对其一共性原因敏感，该割集就是共因目标集。本例中x_1，x_4，x_6，x_3x_{12}，x_2x_{10}，x_2x_{11}等为共因目标集。

由于该法仅分析MCS内各基本事件的相依性，不增大故障树的规模，适宜较复杂系统的相依故障分析。COMCAN程序就按上述原理编制的。

三、参数模型

1．β因子模型[5]

β因子模型是PRA中最早使用的共因故障分析模型之一。该模型中假定每个部件总的故障率λ_I是由独立故障率λ_I和相依故障率λ_C两部分组成的。即

$$\lambda=\lambda_I+\lambda_C \tag{3}$$

β因子定义为：$\beta=\dfrac{\lambda_C}{\lambda_I+\lambda_C}=\dfrac{\lambda_C}{\lambda}$ (4)

参数β的最大似然估计：

$$\beta=\frac{n_C}{n_I+n_C}=\frac{n_C}{n} \tag{5}$$

式中，n为部件总的故障次数；n_I为部件独立故障次数；n_C为部件的相依故障次数。

一般β为0.1数量级或更小，对处在不同环境下的不同部件，β参数值变化甚小，文献[5]指出，类似部件的β值可以相互借用，而不会给结果带来大的影响，这样就可以引用非核工业部门积累的数据分析核系统的相依故障。与Markov模型结合，可导出可修系统的无效度。

2．多种希腊字母模型[6]

简称MGL模型。它是由一批部件级故障率参数组成的，包括对部件故障有贡献的独立和共因作用的影响，是β参数模型近代推广的许多模型中最通用的一个。适宜于分析多个类似或冗余部件间的相依故障(包括启动故障和运行故障)。

MGL模型的参数数目与系统规模的大小有关，系统规模越大，参数数目也越多，而且参数用希腊字母命名。对四个类似的冗余或备用部件A_1—A_4，MGL参数中描述部件启动失败的参数有：

$$\lambda_S=\lambda_{S1}+3\lambda_{S2}+3\lambda_{S3}+\lambda_{S4} \tag{6}$$

$$\beta_S=\frac{3\lambda_{S2}+3\lambda_{S3}+\lambda_{S4}}{\lambda_{S1}+3\lambda_{S2}+3\lambda_{S3}+\lambda_{S4}} \tag{7}$$

$$\gamma_S=\frac{3\lambda_{S3}+\lambda_{S4}}{3\lambda_{S2}+3\lambda_{S3}+\lambda_{S4}} \tag{8}$$

$$\delta_S=\frac{\lambda_{S4}}{3\lambda_{S3}+\lambda_{S4}} \tag{9}$$

式中λ_S为独立和相依事件导致的部件启动失败的故障率；λ_{S1}为因独立故障导致的启动故障率；λ_{S2}为与A_1组合的两个部件(A_1A_2，A_1A_3，A_1A_4)，因相依故障导致的部件A_1启动

失败的故障率；λ_{S3}为与A_1组合的三个部件因相依故障导致的部件 A_1 启动失败的故障率；λ_{S4}为 A_1—A_4四个部件发生相依故障导致部件A_1的启动失败的故障率。如果将上述参数的足标“S”(启动)换成“r”(运行)，就可得到描述部件运行故障的 MGL 参数，即 λ_r，β_r，γ_r和 δ_r。对于两部件冗余系统：

$$\lambda_S=\lambda_{S1}+\lambda_{S2};\quad \beta_S=\frac{\lambda_{S2}}{\lambda_{S1}+\lambda_{S2}}$$

$$\lambda_r=\lambda_{r1}+\lambda_{r2};\quad \beta_r=\frac{\lambda_{r2}}{\lambda_{r1}+\lambda_{r2}}$$

与β因子模型完全一样。

由 m 个部件所组成系统的 MGL 模型，其前三个参数的最大似然估计[7]：

$$\hat{\beta}=\sum_{i=2}^{m} jn_i \Big/ \sum_{i=1}^{m} jn_i;\quad \hat{\gamma}=\sum_{i=3}^{m} jn_i \Big/ \sum_{i=2}^{m} jn_i$$

$$\hat{\delta}=\sum_{i=4}^{m} jn_i \Big/ \sum_{i=3}^{m} jn_i$$

四个冗余部件故障率参数分别为：$\lambda_{S1}=(1-\beta_S)\lambda_S$；$\lambda_{S2}=\frac{1}{3}(1-\gamma_S)\beta_S\lambda_S$；

$\lambda_{S3}=\frac{1}{3}(1-\delta_S)\gamma_S\beta_S\lambda_S$；$\lambda_{S4}=\delta_S\gamma_S\beta_S\lambda_S$

3．两项式故障率模型[8]

简称 BFR 模型，最初是由 Vesely 提出的，属非致命冲击模型。该模型假定非致命冲击对各部件都有影响，每次冲击导致的部件故障数目属两项式分布，故名为两项式故障率模型。在给定的冲击下，BFR 模型假定各部件故障是同时进行的，部件的故障概率不受作用在其它部件上冲击的影响。

更一般化的 BFR 模型是由 Atwood[9]新近提出的，它既包含早期模型的全部特色，也考虑了致命冲击。BFR 模型中含 λ，μ，ω，p 等参数，λ 和 ω 的最大似然估计为

$$\lambda=n_I/mT;\quad \lambda_+=n_+/T;\quad \omega=n_L/T$$

式中 λ 为部件的独立故障率；λ_+为导致至少一个部件故障的非致命冲击率；ω 为致命冲击发生率；n_I为不计致命和非致命冲击时单个部件故障数目；$n_+=\sum_{i=1}^{m} n_i$，其中 n_i为 i 个部件同时故障发生的次数；n_L为致命冲击发生数；m 为系统含的部件数；T 为系统总的运行时间。并由

$$S=\frac{mn_+}{1-(1-p)^m}p;\quad S=\sum_{i=1}^{m} in_i$$

算出 p。其中 p 为给定的非致命冲击下各部件故障的条件概率。μ 为非致命冲击发生率。

$$\mu=\frac{\lambda_+}{1-(1-p)^m}$$

四个冗余部件故障率参数分别为：$\lambda+\mu p$(单个部件)；μp^2(二个部件)；μp^3(三个部件)；$\mu p^4+\omega$(四个部件)。

表 4 相依故障分析模型

Table 4 Modle for the analysis of dependent failure

模型类别	方法	相依故障类型					
		共同触发事件	系统间相依				部件间相依
			功能相依	公用设备	实体作用	人为作用	
显式模型	事件树分析	*	*	*		*	*
	故障树分析	*	*	*	*	*	*
	因果表分析			*	*		*
参数模型	β因子模型						*
	MGL						*
	BFR						*
计算机辅助技术	GO			*	*		*
	WAMCOM, COMCAN BACFIRE, SETS	*		*	*		*

BFR 模型既适用于连续运行期间的相依故障的分析，也可引伸到备用件启动时相依故障的分析。BFR 模型使用条件，仅限于一群受共因作用、故障服从两项式分布或全部故障的部件。

四、结 束 语

表 4 列出了各种模型适用范围。显然，以事件树和故障树为工具的显式模型用途广泛，原则上可用来分析各种类型的相依故障，而且对实体和人为作用是唯一适宜的方法。将相依故障原因直接併入事件树和故障树逻辑模型中，可以清楚地看出系统与共因触发事件间、系统与系统之间、系统内各部件之间的相依关系，有助于人们采取防止相依故障发生的措施。

显模型的局限性在于：(1) 定量计算中涉及到共因触发事件发生条件下部件的故障概率，而计算条件概率的数据是十分缺乏的，所以在早期的 PRA 中用平方根[10]法进行近似的定量计算；(2) 建造定量逻辑模型是极其困难的，要求分析者具有丰富的经验。根据核电站设计资料和运行经验识别的相依故障，只能达到比较合理的完善程度；(3) 一些复杂系统的故障树本身就十分庞大，如再考虑相依故障，有可能使得待处理的割集数目增大到计算机容量和速度达到难以处理的地步。

在可靠性工程中已研制了一批用来分析相依故障的计算机辅助程序，它包括GO,SETS，WAMCOM，BACFIRE 和 COMCAN 程序。GO 和 SETS 程序可用于相依故障的定性和定量分析，其余程序只可作定性分析。这些程序的优点是能根据分析者设想的相依故障原因，有效地寻找系统的薄弱环节。缺点是在运算过程中将产生大量有关相依故障的定量信息，因此，相依故障的任何定量判别是难易实现的。

参数法是通过应用特殊的共因参数定量考虑相依故障的作用。该法仅用来模型故障的相依效应，而不是直接在模型中枚举相依故障发生的原因。应用参数法预测系统相依故障，实际上综合考虑了系统中存在的各种类型的相依事件。象估计部件故障率那样，参数法所用的参数是根据经验数据估计的，发生相依故障的根本原因是隐含在部件故障率测定中。鉴

于参数数模型能定量处理部件间相依故障，所以这些模型大多已在核电站PRA中应用，见表5。

表5 PRA中相依事件处理

Table 5 Treatment of denpendent events in PRA

PRA	完成年份	应用的分析方法
反应堆安全研究[8]	1975	平方根法
HTGR	1976	对所有冗余的有源部件应用β因子模型，根据LWR和GCR运行经验，进行参数定量化
AIPA 研究		
Zion PSA	1978	对选定的部件应用β因子模型
RINGHALS$_2$	1981	对大部分部件应用C因子模型
Seabrock 电站 (PSA)	1983	对所有冗余有三部件以及某些多样性部件采用 MGL 和β因子模型，取自 U.S.A 500 年运行数据

参考文献

[1] Jolly, M. E. et al., *Nuclear Safety*, 18(5), 624(1977).
[2] Fleming, K.N.et al., *Nuclear Safety*, 24(5), 637(1983).
[3] General Electric Co., SRD-75-064,(1978).
[4] Fussell, J. B. et al., ANCR-1273,1976.
[5] Fleming, K. N. et al., GA-A136172,1975.
[6] Pickard et al., PLG-0300, 1983.
[7] Karl, N. et al., *Nuclear Engineering And Design*, 93, 245 (1986).
[8] Steverson J. A. et al., NUREG/CR-2770, 1983.
[9] Atwood, C. L. et al., NUREG/CR-3289, 1983.
[10] U. S. Nuclear Regulatory Commission, WASH-1400, NUREG 75/014, 1975.

（编辑部收到日期：1989 年 3 月 7 日）

OVERVIEW OF DEPENDENT FAILURE ANALYSIS METHODS IN THE PROBABILISTIC RISK ASSESSMENT STUDIES FOR NUCLEAR POWER PLANT

ZHOU FAQIN

(*Shanghai Jiao Tong University*)