第36卷第2期 原 子 能 科 学 技 术 Vol. 36, No. 2
2002年3月 Atomic Energy Science and Technology Mar. 2002

要因防护矩阵定性分析方法在核电厂共因故障分析中的应用

曾满平,赵炳全
(清华大学 核电站模拟培训中心,北京 100084)

摘要:简要介绍了要因防护矩阵定性分析方法,并对核电厂直流电力系统共因故障(CCFs)进行了定性分析。分析表明:提出的防护措施可用于排除、减少或减轻CCFs事件的发生。

关键词:共因故障;要因防护矩阵;根事件;耦合机制
中图分类号:TL361 **文献标识码**:A **文章编号**:1000-6931(2002)02-0178-05

Application of Cause-defense Matrices on Common Cause Failures in Nuclear Power Plant

ZENG Man-ping, ZHAO Bing-quan
(Beijing Nuclear Power Plant Simulation Training Center, Tsinghua University, Beijing 100084, China)

Abstract: The qualitive analysis method on common cause failures (CCFs)/cause-defense matrices is described, and a qualitive analysis on the CCFs probability of DC electric power system in a PWR nuclear power system is given. The analysis results show that the defend measure can be applied to exclude, minish or lighten the probability of CCFs.

Key words: CCFs; cause-defense matrix; root cause; coupling mechanism

直流电力系统的共因故障(CCFs)研究常因没有足够的特定电厂CCFs事件支持,而使用普通的全工业数据。一般工业数据不能直接用于特定电厂的分析,需仔细分析和确定其适用性。

因基于工业数据的分析需要大量的部件知识,如详细的设计参数及运行和维护策略,当利用避免或减轻CCFs来对特定电厂进行防护时,很难确保对事件原因和防护措施评估计算的完整性。另外,一般数据评估计算是确定CCFs事件及分析其直接原因与影响,CCFs的重要特点,如根事件、耦合机制、针对根事件的防护措施及针对耦合机制的防护措施等不能显式表现。要因防护矩阵定性分析结果的一致性和预防的有效性可弥补这些缺陷,它建立在失效事件全面考察的基础上,矩阵列出了需考虑的原因及防护措施,这对确保评估完整性也极其有用。同时,它顾及到更广的深度,从而可改善评估计算。

1 要因防护矩阵模型分析方法

核电厂中安全关联系统均设计有冗余机组

收稿日期:2001-04-24;**修回日期**:2001-10-13
作者简介:曾满平(1976—),男,安徽怀宁人,在读硕士研究生,核能科学与工程专业

设备。实践表明:电厂运行危险只有在这些冗余部件同时达不到设计功能时(多元失效)才会发生。多元失效是部件相关失效的结果。在进行安全和可靠性研究中,通常将大部分的原因(如级联失效、操作失误)显式地包含进事件树/故障树模型中,不适当的设计、生产质量、安装及交付使用中的差错、与维护相关的差错及环境状态(如过湿、易腐蚀或者污染)则不能显式地表现在可靠性模型中。由上述诸多原因形成模型中的一个基本事件,用以表示由这几种原因中的任何一种所造成的多元失效,这样比将它们显式存放要好。CCFs 是产生于不能在模型中显式表示的相关失效和功能失效。

共因故障是由于某种共有的原因造成两个以上部件在同一时刻或在一较短时间间隔内发生相关失效或功能失效。

1.1　失效机制

简单原因即近因(proximate cause)对失效描述往往过于简单。如"高湿导致泵失效"无法阐明湿度为什么高和怎样影响泵,从而无法进行多元失效分析。

为分析失效机制,引入条件事件和触发事件。条件事件是加大共因部件组事故发生概率的潜在因素;触发事件直接触发故障,是失效机制中的动态原因。要因防护矩阵模型中的失效机制往往偏重考虑条件事件。

1.2　根事件

导致部件失效的最基本原因是根事件。建立要因防护矩阵时,最理想的是将防护措施与特定失效根事件直接关联,达到 CCFs 分析的最终目标——预防。然而,当对失效原因考虑得详细时,产生 CCFs 可能的根事件数量将急剧增加。因此,应建立根事件的防护矩阵。

要因防护矩阵模型中的根事件将从共因故障的标准定义出发,以分层结构[1]形式显示,强调某个根事件被引入系统的时间。首先引入设计阶段的那些因素,然后依次是制造安装、交付使用、运行等阶段的具体因素。CCFs 根事件一般与独立失效类同。具体分类如下。1) 设计:需求说明书不够精确、设计说明书错误或不精确。2) 制造:错误或不够精确。3) 安装:错误或不够精确。4) 维护:未遵守规程、有缺陷的程式、管理不适当、团队沟通及培训不够。5) 操作:未遵守规程、有缺陷的程式、管理不适当、团队沟通及培训不够。6) 环境:压力、紧急。

1.3　耦合机制

耦合机制是将独立失效和多元失效分开的真正因素。对电厂各种故障事件诊查表明:一个特定因素(根事件)对多个部件造成影响经常与一种或多种共同状态(耦合机制)相联系,即耦合机制是对同样的失效机制敏感的一组部件或零件的特征,具体包括相同的设计、生产、制造、安装、维护或运行人员及环境位置等。

1.4　措施分析

1.4.1　防护措施的形式　根事件、耦合机制和防护措施构成了要因防护矩阵的基础构架,对应的具体防护措施包括防止产生失效的根事件、耦合机制和两者兼防。在外部根事件的影响下,不同方式的防护措施用于防止冗余部件的多元失效(图 1)。两个冗余部件(A 和 B)受根事件同样的影响(图 1a);防护措施将根事件与冗余部件组隔离,或对根事件进行周期性检修,从而隔离或直接排除根事件,这类措施均帮助两个组件减小独立失效和多元失效的频率,属于对根事件的防护(图 1b);针对耦合机制的防护措施,将两个冗余部件隔离,从而不受根事件同样的影响,该防护措施的重点是减少多元(而非独立)失效频率(图 1c);将防护措施安置在每个部件周围(设备硬化作用),这种措施对根事件和耦合机制皆进行了防护(图 1d)。

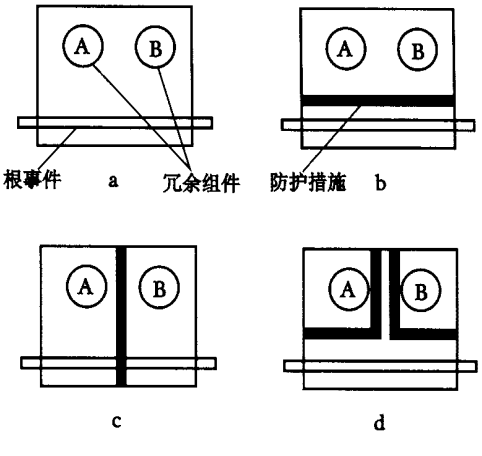

图 1　几种防护措施的形式和作用

Fig. 1　Sample and usage of some defend measures

1.4.2　根事件的防护　CCFs 的根事件与独立失效的根事件没有区别,这在 CCFs 分析中具

有重要意义,它表明对独立失效的防护也可用于 CCFs,即防护措施通常是试图减小独立或多元失效的频率。防护根事件的典型措施[1]包括设计控制、使用环境、测试和预防维护程序、工序的复验、员工的培训及质量控制等。

1.4.3 耦合机制的防护 耦合机制防护的首要内容是相异性,具体防护措施[1]包括:1) 功能、设备和人员的多样性;2) 空间隔离、物理保护、互锁保护、延时或对十字交叉等管理屏障;3) 交叉测试和维护策略;4) 附加冗余性。

1.5 要因防护矩阵模型

由于要因防护矩阵中对根事件和耦合机制的防护往往是较为独立的,因此,一般把防护矩阵分成两个矩阵,分别针对根事件和耦合机制。

1.5.1 建立步骤 实际应用时,要因防护矩阵可按以下步骤建立:1) 熟悉系统,注意组件的类型、冗余分析,建立系统模型;2) 了解历史失效数据,进行机制选定分析,考虑数据的可靠性,列出失效机制表;3) 针对失效数据进行根事件与耦合机制分析,列出根事件和耦合机制表;4) 分析防护措施对根事件的防护能力;5) 分析防护措施对耦合机制的防护能力;6) 建立和细化防护矩阵;7) 进行矩阵的嵌套分析。

1.5.2 要因防护矩阵 要因防护矩阵模型列于表 1。M 为条件事件;D 为防护措施;V_R 和 V_c 为防护措施对应的失效机制的防护有效程度,前者为根事件防护有效性,后者为耦合机制防护有效性;V 为对系统的定性分析值,在很强、较弱、忽略 3 类防护程度的防护矩阵中,可忽略防护作用时,矩阵元取值 0;较弱的防护作用取值 10 %～30 %;很强的防护作用取值为 60 %～90 %。防护矩阵用于更高级别的分析方式时,将应用要因防护矩阵的嵌套矩阵。如,机制 D_i 由 D_{i1}、D_{i2}、D_{i3} 组成,对应事件和耦合机制超过 1 个,防护措施可进一步细化。

1.6 要因防护矩阵的计算和分析

要因防护矩阵清楚地描绘了对根事件和耦合机制的不同防护措施作用。一些防护侧重于防护根事件的发生,另一些防护侧重于对耦合机制的预防,其它的防护可对两者均有影响。防护能力可按下式计算得出。

防护措施的防护能力为:

$$D_i = \sum_{j=1}^{n} P_{m_i} \times V_R(j,i) + \sum_{j=1}^{n} P_{m_i} \times V_c(j,i) \quad (1)$$

失效机制的失效能力为:

$$M_j = \sum_{i=1}^{n} P_{D_i} \times V_R(j,i) + \sum_{i=1}^{n} P_{D_i} \times V_c(j,i) \quad (2)$$

根事件的防护有效性为:

$$R_i = \sum_{j=1}^{n} P_{M_j} \times V_R(j,i) \quad (3)$$

耦合机制的防护有效性为:

$$C_i = \sum_{j=1}^{n} P_{M_j} \times C_R(j,i) \quad (4)$$

其中:D_i 为第 i 个防护措施的防护能力;M_j 为第 j 个失效机制的失效总体能力值;R_i 为系统对第 i 个根事件的防护能力值;C_i 为系统对第 i 个耦合机制的防护能力值;P_{M_j} 为第 j 个失效机制的概率;V_R、V_c 分别为根事件和耦合机制的相应防护有效程度。

表 1 要因防护矩阵模型

Table 1 Model of cause-defend matrix

条件事件	防护措施							
	D_1		D_2		$D\cdots$		D_n	
M_1	$V_R(1,1)$	$V_c(1,1)$	$V_R(1,2)$	$V_c(1,2)$	$V_R(1,\cdots)$	$V_c(1,\cdots)$	$V_R(1,n)$	$V_c(1,n)$
M_2	$V_R(2,1)$	$V_c(2,1)$	$V_R(2,2)$	$V_c(2,2)$	$V_R(2,\cdots)$	$V_c(2,\cdots)$	$V_R(2,n)$	$V_c(2,n)$
$M\cdots$	$V_R(\cdots,1)$	$V_c(\cdots,1)$	$V_R(\cdots,2)$	$V_c(\cdots,2)$	$V_R(\cdots,\cdots)$	$V_c(\cdots,\cdots)$	$V_R(\cdots,n)$	$V_c(\cdots,n)$
M_n	$V_R(n,1)$	$V_c(n,1)$	$V_R(n,2)$	$V_c(n,2)$	$V_R(n,\cdots)$	$V_c(n,\cdots)$	$V_R(n,n)$	$V_c(n,n)$

2　应用实例——直流电力系统定性分析[2,3]

直流电力系统的逻辑模型示于图2。

2.1　防护矩阵的失效机制

本例考虑厂用蓄电池失效或电池功能无效等较为重要的机制(表2中的第1列)。

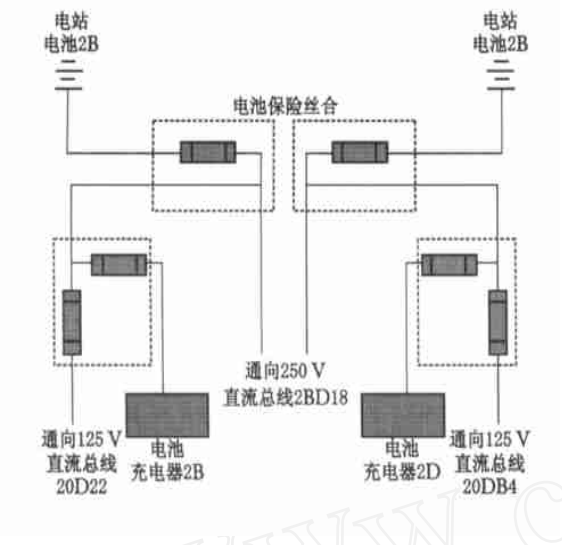

图2　125/250 V直流电力系统示意图

Fig. 2　Sketch of 125/250 V DC electric power system

2.2　根事件的防护分析

表2为选定电池失效机制的要因防护矩阵,所选的防护措施包括了防止厂用蓄电池失效机制的方案。

电池内部故障或与终端连接部件相联系的故障导致电池失效。终端连接部件故障一般由连接表面的腐蚀产生或由安装夹持器产生的不适当扭矩所造成。大多数内部故障表现为逐渐的退化作用,它们与电解液、铅板、活性材料、容器罩或其它退化原因有关。这些退化进程缓慢增大到导致严重失效或电池性能剧减。这种退化进程一般可由观察和试验发现。

对内部故障或终端连接部件故障的有效防护方法是扩充一般检查,因它涉及检验和记录每个电池的质量、电压和总电池组的终端电压及典型电池中电解液的温度。一般检查只要求检验和记录指示用电池的电压、特定质量和温度,所以,不能达到扩充检查的效果。

容量测试(性能测试或保养测试)在检测内部故障及终端连接部件故障中非常有效,但它通常只在初始安装和充电时才进行,与扩充一般检查相比,允许更长时间(前者通常每年至少需要4次)。因这些失效机制将导致严重失效或电池性能剧减,因此,一般检查和容量检查不是重要的防护措施。

2.3　耦合机制的防护分析

表3所列为针对耦合机制进行防护的要因防护矩阵,它包括设备和人员多样性、空间分隔、交错检查、测试与维护(补偿充电)。

表2　要因防护矩阵防护措施对电厂电池失效根事件的影响

Table 2　Influence of measures in cause-defend matrix on root cause of battery failure in power plant

电厂电池失效或功能不可用的选定失效机制	对电厂电池失效或功能不可用的根事件防护措施						
	控制室报警设备		检查和测试			补偿模式下设计和控制参数	
	总线电压	电池CB状态	一般检查	扩充一般检查措施	容量测试	完全自动	在线补偿充电
内部缺陷或与终端连接相关的缺陷	0	0	0	0.9	0	0	0
由于直流电力总线上非正常高压导致的保险丝熔断	0.9	0	0.2	0	0	0	0
保险丝假象开路	0	0	0	0	0.2	0	0
电池CB的假象开路(CB的硬件失效或操作人员的错误)	0	0.8	0.2	0	0	0	0.9
紧随电池损耗或电池容量测试的不合适的充电(包括操作人员没有充电)	0	0	0.2	0	0	0.9	0
过压充电的损坏	0	0	0.2	0	0	0.9	0
火和其他紧急事件的破坏	0	0	0	0	0	0	0

表3 要因防护矩阵防护措施对电厂电池失效耦合机制的影响

Table 3 Influence of measures in cause-defend matrix on coupling mechanism of battery failure in power plant

电厂电池失效或功能不可用的选定失效机制	对电厂电池失效或功能不可用的根事件防护措施						
	多样性		空间隔离	测试与维护策略			
	设备	人员		交错一般测试	交错扩充一般测试	交错容量测试	交错补偿充电
内部缺陷或与终端连接相关的缺陷	0.9	0.9	0	0	0.2	0	0
由于直流电力总线上非正常高压导致的保险丝熔断	0	0	0	0.2	0	0	0
保险丝假象开路	0	0	0.2		0	0.2	0
电池CB的假象开路(CB的硬件失效或操作人员的错误)	0	0.9	0	0.2	0	0	0
紧随电池损耗或电池容量测试的不合适的充电(包括操作人员没有充电)	0	0.9	0	0.2	0	0.9	0
过压充电的损坏	0	0.9	0.2	0.2	0	0.2	0.2
火和其他紧急事件的破坏	0	0	0.9	0	0	0	0

内部故障或与终端连接部件相关的故障表现为逐渐的退化作用,但对多样性的设备,一般不会以同样的方式和速度退化,因此,设备多样性是针对耦合机制的强有力的防护措施。由于内部故障或与终端连接部件相关的故障将导致失效检修和维护工作,也可涉及人为错误(委托或遗漏),因此,如表3所述,人员多样性对降低与电池失效很多相关的耦合机制也很重要。显然,如果错误不是由不正常的工序产生,不同的工作人员以同样方式犯错误的可能性很小。交错进行的检修和测试与同时或连续进行相比较,提供了针对耦合机制的一些保护措施。首先,它减小了与人有关的耦合失效。因当工作以月、周、天进行时,技术人员的误操作比以分钟或小时进行时减少。交错进行检修和测试的第2个优点在于涉及到CCFs事件的持续时间。如果多组电池因内部故障或与终端连接部件相关的故障而失效,在不增加对单独电池的检修和测试次数的情况下,平均的交错检修和测试则可减小多组电池失效的最大时间。

3 结 论

本文针对要因防护矩阵定性分析方法提出了一个对防护措施的可察觉作用和效果的评估体系,这些防护措施用于排除、减少或减轻CCFs事件的发生。通过定性要因防护矩阵的建立,可扩展当前条件下的CCFs分析技术,包括:1) 提供减少CCFs可能性的定性信息;2) 通过特定电厂的评估计算的防护措施改善CCFs分析的深度和质量;3) 通过特定部件要因防护矩阵改善CCFs分析的深度和质量;4) 通过可察觉的普遍数据信息达到CCFs分析的一致性;5) 允许CCFs分析与PRAs更为显式地表达,用以确定特定电厂的设计参数及运行和维护策略。

参考文献:

[1] Mosleh A, Fleming KN, Parry GW, et al. Procedures for Treating Common Cause Failures in Safety and Reliability Studies: Vol Ⅰ, Ⅱ[R]. California: Electric Power Research Institute, Palo Alto, 1989.

[2] Paula HM, Campbell DJ. Task 5 Draft Report: a Cause-defense Methodology for Common Cause Failure Analysis[R]. Tennessee: JBF Associates, Inc, Knoxville, 1988.

[3] Paula HM, Parry GW, Campbell DJ, et al. A Cause-defense Approach to the Understanding and Analysis of Common Cause Failures[R]. New Mexico: Sandia National Laboratories, Albuquerque, 1990.